ISO/IEC JTC 1/SC 37 Biometrics

Document Type: WD Text

Document Title: Text of Standing Document 2 (SD 2) Version 8, Harmonized Biometric Vocabulary

Source: Project Editor

Document Status: As per Berlin resolution 1.2, this document is circulated to SC 37 National Bodies for review and comment. Comments received by 15 November 2007 will be considered at the January 2008 WG 1 meeting in Israel.

In preparation for review of the received comments at the January 2008 WG 1 meeting, the Project Editor is instructed to prepare, by 29 November 2007, a summary of comments document, including a proposed Editor’s disposition of each comment. This Editor’s document will serve as the basis for discussion at the January 2008 meeting.

Action ID: Comments

Due Date: 15 November 2007

No. of Pages: 98
ISO/IEC JTC1/SC 37 Standing Document 2 — Harmonized Biometric Vocabulary

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.
Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO’s member body in the country of the requester:

[Indicate the full address, telephone number, fax number, telex number, and electronic mail address, as appropriate, of the Copyright Manager of the ISO member body responsible for the secretariat of the TC or SC within the framework of which the working document has been prepared.]

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.
C.8.5 Concept map from previous version of SD2 – use when developing "Interacting" concept map ............................................................................................................................61
C.8.6 Concept map from previous version of SD2 – use when developing "Interacting" concept map ............................................................................................................................62
C.9 Personnel.................................................................................................................. .................................63
C.9.1 Subjects................................................................................................................. ............................64
C.9.2 General .................................................................................................................. ............................66
C.10 Application .............................................................................................................. .................................68
C.10.1 Application 1 ........................................................................................................... ..........................68
C.10.2 Application 2 ........................................................................................................... ..........................69
C.11 Performance ........................................................................................................... .................................70
C.11.1 Performance 1 (working slide) ........................................................................................... ..............70
C.11.2 Performance 2 (working slide) ........................................................................................... ..............71
C.11.3 Performance 3 ........................................................................................................... ..........................72
C.11.4 Performance 4 ........................................................................................................... ..........................73
C.11.5 Performance 5 ........................................................................................................... ..........................74
C.11.6 Performance 6 ........................................................................................................... ..........................75
C.11.7 Performance 7 ........................................................................................................... ..........................76
C.11.8 Performance 8 ........................................................................................................... ..........................77
C.11.9 Performance 9 ........................................................................................................... ..........................78
C.11.10 Performance 10 .........................................................................................................................79
C.11.11 Performance 11 .........................................................................................................................80
C.12 Quality................................................................................................................... .............................81
Annex D (informative) Priority terms list .......................................................................................82
Bibliography ................................................................................................................... ................................87
Alphabetical Index ............................................................................................................. ............................88
Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National Bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 2 was prepared by Technical Committee ISO/TC JTC1, Information Technology, Subcommittee SC 37, Biometrics.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.
Introduction

The main purpose of this international terminology standard is to provide a systematic description of the concepts in the subject field of biometrics and to clarify the use of the terms in this subject field. The subject field of biometrics is broken down into sub-fields.

The compilation of this vocabulary provides a forum for analysing, discussing and coordinating key concepts found in ISO/IEC JTC1 SC 37 standards. This International Standard is addressed to biometrics standardizers, and to users of these standards.

Terms defined in this document are to be understood in the subject field of biometrics. When terms exist in various subject fields, the current subject field may be indicated in parenthesis.

EXAMPLE

candidate
<biometrics> identifier of a biometric reference in the enrolment database determined to be similar to the recognition biometric sample

candidate
<politics> a person who applies for a job or is nominated for election

Note: When using terms defined with a qualifier (for example, “biometric xxx”), it should be normal to include the qualifier on the first occurrence of the term in every paragraph, but to omit it on subsequent occurrences of that term within the same paragraph.

The terms in this International Standard are listed in a systematic order under a number of general headings.

The notation used in the notes throughout this International Standard is as follows:

- Concepts are indicated by single quotes;
- Designations (terms or appellations) are in bold font;
- Characteristics are underlined;
- Types of characteristics are doubly underlined.

The alphabetical index includes preferred and admitted terms.

Annex A contains concept diagrams which represent the relations among the concepts defined in the vocabulary.

Information within this document is undergoing development by ISO/IEC JTC1 SC37 WG1. The following conventions are used within this document:
Text that is indicated that the term/definition has not yet been harmonized within WG1, otherwise the term/definition is harmonized and its use is encouraged within ISO/IEC JTC1 SC37 projects.

The presence of a term with no definition implies that this term is considered to be included in the sub-field, and that the concept represented by this term will be developed by WG1.

Some terms may appear in more than one clause. This implies that WG1 has not agreed upon which is the proper sub-field delimation for the concept represented by that term. The alternate sub-fields will be noted in square brackets following the term.

Deprecated terms as their own clause need to be removed before publication of this document as this format does not follow ISO rules.

Reference numbers following concepts to be reinserted before publication of this document as this is required by ISO rules.

Standing Document 2 — Harmonized Biometric Vocabulary

1 Scope

This standing document establishes a systematic description of the concepts in the field of biometrics pertaining to recognition of human beings and reconciles variant terms use in pre-existing biometric standards against the preferred terms, thereby clarifying the use of terms in this field.

Excluded from the scope of this document are concepts (represented by terms) from information technology, pattern recognition, biology, mathematics, etc. Biometrics uses such fields of knowledge as a basis.

In principle, modality-specific terms are outside of scope of this standing document.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 704:2000, Terminology work – Principles and methods

ISO 860:1996, Terminology work – Harmonization of concepts and terms


ISO 2382-17:1999, Information technology – Vocabulary – Part 17: Databases

3 Biometric vocabulary

This document establishes terminology in the subject field of biometrics.

3.1 General concepts

3.1.1 biometric (adj.)
of or having to do with biometrics

NOTE The use of biometric as a noun, to mean for example, biometric characteristic, is deprecated.

EXAMPLE Incorrect usage #1: ICAO resolved that face is the biometric most suited to the practicalities of travel documents.

EXAMPLE Correct usage #1: ICAO resolved that face recognition is the biometric modality most suited to the practicalities of travel documents.

EXAMPLE Incorrect usage #2: The biometric recorded in my passport is a facial image.

EXAMPLE Correct usage #2: The biometric characteristic recorded in my passport is a facial image.

3.1.2 biometric algorithm

3.1.3 biometric modality

3.1.4 biometric mode (noun), modal (adj)

3.1.4.1 multi/biometric

3.1.4.1.1 multimodal

3.1.4.1.2 multialgorithmic

3.1.4.1.3 multisensory

3.1.4.1.4 multipresentation

3.1.4.2 unimodal
3.1.5  
**biometrics**  
automated recognition of **individuals** based on their behavioural and biological characteristics

NOTE 1  "**Individual**" is restricted in scope by SC37 to humans.

NOTE 2  The general meaning of biometrics encompasses counting, measuring and statistical analysis of any kind of data in the biological sciences including the relevant medical sciences.

3.2 Biometric system

3.2.1  Biometric system components

3.2.1.1  **biometric product**

3.2.1.2  **biometric system**  
system for the purpose of the automated recognition of **individuals** based on their behavioural and biological characteristics

3.2.1.3  **verification system**  
system which performs biometric verification

3.2.2  Data in biometric systems

3.2.2.1  Biometric data and non-biometric data overlapping concepts

3.2.2.1.1  **biometric enrolment database**

3.2.2.1.2  **data object**  
discrete data, considered as a unit, representing an instance of a data structure that is known or assumed to be known

NOTE  Definition source: ISO 2382-17, term 17.01.11

3.2.2.1.3  **record (in databases)**  
**data object** that is an instance of a record type

NOTE  Definition source: ISO 2382-17, term 17.05.12

3.2.2.1.4  **enrolment data record**  
**record** created upon **enrolment**, associated with the **biometric data subject** and including **biometric reference(s)** and typically non-biometric data
3.2.2.2 Biometric data terms

3.2.2.2.1 biometric characteristic
biometric (deprecated)
biological and behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals

NOTE 1 Biological and behavioural characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these.

NOTE 2 Distinguishing does not necessarily imply individualization.

EXAMPLE Examples of biometric characteristics are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, etc.

3.2.2.2.2 biometric data
biometric sample at any stage of processing, biometric reference, biometric feature or biometric property

3.2.2.2.3 Biometric Data Block (BDB)
block of data with a defined format that contains one or more biometric samples or biometric templates

NOTE Definition according to CBEFF.

3.2.2.2.4 biometric feature
numbers or labels extracted from biometric samples and used for comparison

NOTE 1 Biometric features are the output of a completed biometric feature extraction process.

NOTE 2 The use of this term should be consistent with its use by the pattern recognition and mathematics communities.

NOTE 3 A biometric feature set can also be considered a processed biometric sample.

3.2.2.2.5 Biometric Information Record (BIR)
data structure containing one or more BDBs together with information identifying the BDB formats, and possibly further information such as whether the BDB is encrypted

NOTE Definition according to CBEFF.

3.2.2.2.6 biometric property
descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means

EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow, i.e. arch, whorl, and loop types; In the case of facial recognition, this could be estimates of age or gender.

3.2.2.2.7 biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison

EXAMPLE Face image on a passport; Fingerprint minutiae template on a National ID card; Gaussian Mixture Model, for speaker recognition, in a database.
NOTE A biometric reference may be created with implicit or explicit use of auxiliary data, such as Universal Background Models.

3.2.2.2.7.1 biometric model
stored function (dependent on the biometric data subject) generated from a biometric feature(s)

NOTE 1 Comparison applies the function to the biometric features of a recognition biometric sample to give a comparison score.

NOTE 2 The function may be determined through training.

NOTE 3 A biometric model may involve intermediate processing similar to biometric feature extraction.

EXAMPLE Examples for the stored function could be a Hidden Markov Model, Gaussian Mixture Model or an Artificial Neural Network.

3.2.2.2.7.2 biometric template
set of stored biometric features comparable directly to biometric features of a recognition biometric sample

NOTE 1 A biometric reference consisting of an image, or other captured biometric sample, in its original, enhanced or compressed form, is not a biometric template.

NOTE 2 The biometric features are not considered to be a biometric template unless they are stored for reference.

3.2.2.2.8 biometric sample
analog or digital representation of biometric characteristics prior to biometric feature extraction process and obtained from a biometric capture device or biometric capture subsystem

NOTE A biometric capture device is a biometric capture subsystem with a single component.

3.2.2.2.8.1 captured biometric sample
raw biometric sample (deprecated) biometric sample that is output of biometric capture process

3.2.2.2.8.2 intermediate biometric sample
biometric sample that is output of intermediate biometric sample processing

EXAMPLE Intermediate biometric samples may have been enhanced for biometric feature extraction, compressed for compact storage purposes, etc.

3.2.2.2.9 probe (deprecated) / recognition biometric sample, etc?

3.2.2.2.10 recognition

3.2.2.2.11 reference maturity
3.2.2.3 Non-biometric data

3.2.2.3.1 Non-biometric data produced in biometric processing

3.2.2.3.1.1 biometric reference identifier
pointer to a biometric reference in the enrolment database

3.2.2.3.1.2 candidate
biometric reference identifier in the enrolment database determined to be similar to the recognition biometric sample

NOTE Determination may be on the basis of comparison score and/or rank.

3.2.2.3.1.3 candidate list
set of zero, one or more candidates that may be intermediate or final

NOTE Intermediate candidate lists may be produced by systems that use multi-pass biometric identification (3.2.4.1.2).

3.2.2.3.1.4 candidate score
comparison score for a candidate

3.2.2.3.1.5 comparison score
matching score (deprecated)
numerical value (or set of values) resulting from a comparison

NOTE Higher is not meant to mean more similar.

3.2.2.3.1.5.1 distance score / dissimilarity score
comparison score that decreases with similarity

3.2.2.3.1.5.2 similarity score
comparison score that increases with similarity

3.2.2.3.1.6 comparison decision
determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies) including a threshold, and possibly other inputs

NOTE 1 A match is a positive comparison decision.

NOTE 2 A non-match is a negative comparison decision.

NOTE 3 A decision of "undetermined" may sometimes be given.

3.2.2.3.1.7 match (n)
comparison decision that the recognition biometric sample(s) and the biometric reference are from the same source
3.2.2.3.1.8
non-match (n)
comparison decision that the recognition biometric sample(s) and the biometric reference are not from the same source

3.2.2.3.1.9
matching score (deprecated)
NOTE This term is deprecated in favour of comparison score.

3.2.2.3.2 Non-biometric data associated with a biometric data subject, a biometric sample or a biometric reference

3.2.2.3.2.1
biometric data log

3.2.2.3.2.2
biometric sample metadata

3.2.2.3.2.3
claimed identity
reference in a biometric enrolment database to which an assertion is made that a biometric capture subject is the source
NOTE Usually made in the first person.

3.2.2.3.2.4
ground truth

3.2.2.3.2.5
individual metadata

3.2.2.3.3 Non-biometric data associated with administration

3.2.2.3.3.1 Decision policy

3.2.2.3.3.1.1
acceptance

3.2.2.3.3.1.2
decision policy

3.2.2.3.3.1.3
rejection

3.2.2.3.3.1.4
threshold
3.2.2.3.3.2 Signal processing parameters and environment conditions

3.2.2.3.4 Privacy and biometric data not associated with a Person

3.2.3 Devices

3.2.3.1 biometric capture device
device that collects a signal from a biometric characteristic and converts it to a captured biometric sample

NOTE 1 A signal can be generated by the biometric characteristic or generated elsewhere and affected by the biometric characteristic, for example, face illuminated by incident light.

NOTE 2 A device can be any piece of hardware (and supporting software and firmware).

NOTE 3 A biometric capture device may comprise components such an illumination source, one or more biometric sensors, etc.
3.2.4 Functioning

3.2.4.1 Comparison family

3.2.4.1.1 biometric application decision

Conclusion based on the application decision policy after consideration of one or more comparison decisions, comparison scores and possibly other non-biometric data.

NOTE 1 Biometric application decisions can be made on the basis of complex policies, allowing for variable numbers of positive comparison decisions.

NOTE 2 A biometric verification (3.5.4) application could allow a positive biometric application decision even if there are one or more non-matches against enrolled biometric references.

EXAMPLE A biometric application decision could be “accept claim”.

3.2.4.1.2 biometric identification (biometric system function) (outlined as definition must be re-addressed – see concept map)

Biometric system function that performs a one-to-many comparison to obtain a candidate list.

EXAMPLE BioAPI_IdentifyMatch

NOTE A biometric identification function may be used to verify a claim of enrolment in an enrolment database without a specified biometric reference identifier.

3.2.4.1.3 biometric verification (biometric system function) (outlined as definition must be re-addressed – see concept map)

Authentication (deprecated)

Positive identification (deprecated)

Biometric system function that performs a one-to-one comparison.

EXAMPLE BioAPI_VerifyMatch

NOTE A biometric identification application (3.5.3) can use an exhaustive series of biometric verification function calls.

3.2.4.1.4 comparison

Match / matching (n) (deprecated as a synonym for comparison)

Estimation, calculation or measurement of similarity or dissimilarity between recognition biometric sample(s) / biometric features / biometric models and biometric reference(s).

NOTE 1 Compare (v) – estimate, measure or note the similarity or dissimilarity between.

NOTE 2 Match (v) is deprecated as a synonym to compare (v).
3.2.4.1.5
**one-to-one comparison**

process in which a recognition biometric sample / biometric feature / biometric model set from one biometric data subject is compared to biometric reference(s) to produce a comparison score with respect to one biometric data subject, perhaps using additional data from the enrolment database.

**NOTE 1** A biometric verification (3.2.4.1.3) function performs a one-to-one comparison.

**NOTE 2** In the case of a multimodal biometric system, the recognition biometric sample / biometric feature / biometric model, the biometric reference and possibly the comparison score in the above definition comprise components for each biometric modality.

**NOTE 3** In the case of likelihood-ratios, calculation will involve comparisons determining the consistency of the recognition biometric sample / biometric feature / biometric model set of one biometric data subject with the biometric reference(s) of many biometric data subjects. Nevertheless the comparison score generated refers to the similarity between a recognition biometric sample / biometric feature / biometric model set of one biometric data subject and a biometric reference of one biometric data subject, therefore the process is considered a one-to-one comparison.

**NOTE 4** A comparison can still be considered one-to-one even if a universal background model or cohort models are used.

Editor's note: Editor was tasked (in London) to look into the rules for using quotation marks (to see if we can represent the term as "one-to-one" comparison to indicate "one-to-one" is a cliché). ISO 704 and 1087-1 both use quotation marks to identify concepts throughout the document. However, there are no rules for using quotation marks within a vocabulary standard. Suggest we use the quotation marks for "one-to-one" and include a note (either here or in the Introduction) to indicate the use of the quotation marks throughout this document is to identify clichés.

3.2.4.1.6
**one-to-few (deprecated)**

NOTE One-to-few has previously been used to describe the processes of (a) a one-to-many comparison of part of the enrolment database, for example, searching a binning partition; (b) a set of one-to-one comparisons against a set of biometric references for one biometric data subject, or for one claimed biometric reference identifier.

3.2.4.1.7
**one-to-many comparison**

one-to-few (deprecated)

process in which a recognition biometric sample / biometric feature / biometric model set of one biometric data subject is compared against the biometric references of more than one biometric data subject to return a set of comparison scores.

**NOTE 1** A biometric identification (3.2.4.1.2) function performs a one-to-many search.

**NOTE 2** In the case of a multimodal biometric system, the recognition biometric sample / biometric feature / biometric model and the biometric reference in the above definition comprise individual biometric samples / biometric feature / biometric model and biometric references of the component modalities.

**NOTE 3** A universal background model is not associated with a biometric data subject, therefore a comparison of a single biometric data subject's sample to a claimed reference and a universal background model is not inherently one-to-many. In other words, use of a universal background model can still be one-to-one.

3.2.4.1.8
**thresholding / cull / exclude**

elimination of biometric reference identifier(s) associated with biometric reference(s) and/or identifiers for recognition biometric sample(s) that have failed to attain a level of any type of score.

**NOTE** Score can be quality score, comparison score, etc.
3.2.4.2 Data management terms

3.2.4.2.2 deactivate

3.2.4.2.5 loading biometric reference

3.2.4.2.6 reactivate

3.2.4.3 Data capture family

3.2.4.3.1 biometric capture process
process of collecting or attempting to collect signals from a biometric characteristic and converting them to a captured biometric sample

NOTE 1 A signal can be generated by the biometric characteristic or generated elsewhere and affected by the biometric characteristic. For example, face illuminated by incident light.

NOTE 2 Each signal collected could stem from a different presentation.

NOTE 3 The biometric capture process may involve a single biometric capture device. In other systems the capture may be distributed over time and space in such a way that there is no single definable biometric capture device.

3.2.4.3.2 biometric capture subsystem
biometric capture device(s) and sub-processes required to execute a biometric capture process

EXAMPLE In some systems, converting a signal from a biometric characteristic to a biometric sample may include multiple components such as a camera, photographic paper, printer, digital scanner, ink and paper.

3.2.4.3.3 capture (function call) [also in Interacting]

3.2.4.3.4 Instructions and subject feedback

3.2.4.3.5 last point of transduction

3.2.4.3.6 physical factors that impact data capture conditions

3.2.4.3.7 presentation [also in Interacting]

3.2.4.3.7.1 cooperative presentation
3.2.4.3.7.2
explicit presentation

3.2.4.3.7.3
frontal presentation

3.2.4.3.7.4
implicit presentation

3.2.4.3.7.5
right side presentation

3.2.4.3.7.6
left side presentation

3.2.4.3.7.7
uncooperative presentation

3.2.4.3.8
subject interface

3.2.4.4  Enrolment family

3.2.4.4.1
biometric reference adaptation
automatic incremental updating of a biometric reference to mitigate performance degradation

NOTE For example, degradation may be from minor changes in the biometric characteristic, channel or sensor.

3.2.4.4.2
biometric reference renewal

3.2.4.4.3
de-enrolment

3.2.4.4.4
duplicate enrolment check
comparison of a recognition biometric sample / biometric feature / biometric model to some or all of the biometric references in the enrolment database to determine if any similar biometric reference exists

3.2.4.4.5
end result of enrolment
3.2.4.4.6 enrol
create and store, for a biometric capture subject, an enrolment data record associated with that biometric capture subject and including biometric reference(s) and, typically, non-biometric data

3.2.4.4.7 enrolment registration (deprecated)
the action of enrolling or being enrolled

3.2.4.4.8 re-enrolment
process of establishing a new biometric reference for a biometric data subject already enrolled in the database

NOTE 1 Re-enrolment requires new captured biometric sample(s).

NOTE 2 For example, re-enrolment may be required as a result of performance degradation due to major changes in the system or biometric characteristics.

3.2.4.5 Signal processing family

3.2.4.5.1 biometric feature extraction process
process applied to a biometric sample with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other biometric samples

NOTE 1 Filters applied to biometric samples are not themselves biometric features, however the output of the filter applied to these samples may be. Therefore, for example, eigenfaces are not biometric features.

NOTE 2 Repeatable implies low variation between outputs generated from biometric samples of the same biometric data subject.

NOTE 3 Distinctive implies high variation between outputs generated from biometric samples of different biometric data subjects.

NOTE 4 An uncompleted biometric feature extraction process might be an error message or a NULL vector.

3.2.4.5.2 decryption
reversal of a corresponding encryption

NOTE Definition source: ISO 18033-1 (via SC27 SD6).

3.2.4.5.3 encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data. [ISO/IEC 18033-1]

NOTE Definition source: ISO 18033-1 (via SC27 SD6)

3.2.4.5.4 intermediate biometric sample processing
any manipulation of a biometric sample that does not produce biometric features

EXAMPLE Examples of intermediate biometric sample processing include cropping, down-sampling, compression, conversion to data interchange formats standard and image enhancement.
3.3 Interacting

3.3.1 attack

3.3.1.1 active attack

3.3.1.2 passive attack

3.3.2 attempt

3.3.2.1 genuine verification attempt

3.3.2.2 imposter verification attempt

3.3.3 attended operation

3.3.4 biometric claim

claim that a biometric capture subject is or is not the source of a specified or unspecified biometric reference

NOTE 1 A biometric claim can be made by any user of the biometric system.

NOTE 2 The phrase "claim of identity" is often used to label this concept.

NOTE 3 Claims may be positive – i.e. that the biometric capture subject is enrolled; negative – i.e. that the biometric capture subject is not enrolled, specific – i.e. that the biometric capture subject is or is not enrolled as a specified biometric enrollee; or non-specific – i.e. that the biometric capture subject is or is not among the set or subset of biometric enrollees.

NOTE 4 Biometric claims are not necessarily made by the subject.

NOTE 5 The biometric reference could be on a database, card or distributed throughout a network.

3.3.4.1 affirmed biometric claim

3.3.4.2 denied biometric claim

3.3.4.3 fraudulent biometric claim
3.3.4.4
negative biometric claim

3.3.4.5
positive biometric claim

3.3.5
live capture

3.3.6
presentation [also in Data capture family]

3.3.7
session

3.3.8
transaction

3.3.8.1
genuine verification transaction

3.3.8.2
imposter verification transaction

3.3.9
trial

3.4 Personnel

3.4.1 Subjects

3.4.1.1
biometric capture subject
individual who is the subject of a biometric capture process

NOTE The subject remains a biometric capture subject only during the biometric capture process.

3.4.1.2
biometric data subject
individual whose individualized biometric data is within the biometric system

NOTE The intent of the word “individualized” is to distinguish biometric data subjects from those whose aggregated data was used in the creation of the biometric recognition algorithm. Examples of individuals contributing biometric data who are not biometric data subjects include those who contributed to a Universal Background Model in speaker recognition systems, or who contributed to the creation of an eigenface basis set in a facial recognition system.

3.4.1.3
subversive user
user of a biometric system who attempts to subvert the correct and intended system policy
EXAMPLEs Operator letting unsanctioned subject through, users initiating denial of service attack, administrators allowing unsanctioned function creep, subjects impersonating enrolled users.

3.4.1.3.1 subversive capture subject
subversive user who is a data capture subject

3.4.1.3.1.1 impostor
person who assumes a false identity in order to deceive or defraud (Oxford)

3.4.1.3.1.2 Identity concealer
alter the appearance, sound, taste or smell of so as to conceal the identity (Oxford)

3.4.2 General

3.4.2.1 attendant
agent of the biometric system operator who directly interacts with the biometric capture subject

EXAMPLE An immigration officer supervising biometric capture process and taking action on the comparison decision.

3.4.2.2 biometric enrollee
biometric data subject whose biometric data is held in a biometric enrolment database

3.4.2.3 biometric system operator
person(s) who executes policies and procedures in the administration of a biometric system

3.4.2.4 biometric system owner
person(s) with overall accountability for the acquisition, implementation and operation of the biometric system

3.4.2.5
client

3.4.2.6 end user (deprecated)
NOTE “End user” suggests active involvement and could be confused with biometric system owner, biometric system operator, administrator, biometric subject.

3.4.2.7 user (of a biometric system)
any person or organization interacting in any way with a biometric system

NOTE When discussing a particular class of users involved with biometric systems, the specific term for that class should be used. For example, those users whose biometric data is being collected should be referred to as biometric capture subjects.

3.5 Application

3.5.1 application (outlined as definition must be re-addressed – see concept map)
program or piece of software designed to fulfil a particular purpose
NOTE This dictionary definition does not preclude other natural language use of the term “application” in the context of biometrics, for example, biometric samples might be collected from a biometric capture subject during an application for a passport or visa.

3.5.2 authentication
NOTE 1 Use of this term as a synonym for “biometric verification or biometric identification” is deprecated; the term biometric recognition is preferred.

NOTE 2 This term has been used in as a synonym primarily for: biometric verification (3.5.4) application, biometric verification (3.2.4.1.3) function, but also as a synonym for biometric identification application (3.5.3) and biometric identification (3.2.4.1.2) function.

3.5.3 biometric identification application
system which contains an open-set or closed-set identification application

3.5.4 biometric recognition

3.5.5 biometric verification (biometric application)
authentication (deprecated) application that shows true or false a claim about the similarity of biometric reference(s) and recognition biometric sample(s) by making a comparison(s)

EXAMPLE Establishing the truth of any of the claims “I am enrolled as biometric data subject X”, “I am enrolled in the database as an administrator”, “I am not enrolled in the database”, may be considered verification.

NOTE A claim of enrolment in a database without declaring a specific biometric reference identifier may be verified by exhaustive search.

3.5.6 closed-set identification (biometric application)
application that ranks the biometric references in the enrolment database in order of decreasing similarity against a recognition biometric sample

NOTE 1 Closed-set identification always returns a non-empty candidate list.

NOTE 2 Closed-set identification is rarely used within practical systems, but is often used experimentally.

3.5.7 identify
the act of making a series of comparisons against an enrolment database to find and return the biometric reference identifier(s)

NOTE This may be performed by using comparison scores, thresholds and decision policies.

3.5.8 negative identification (deprecated)
NOTE 1 Use of this term is deprecated to avoid confusion between biometric verification (3.2.4.1.3) and biometric identification (3.2.4.1.2)

NOTE 2 This term has been used in biometrics to mean biometric verification (3.5.4) of a claim to not be the source of any biometric reference in the database

NOTE 3 Preferred expression would be a negative identity claim.
3.5.9 **open-set identification (biometric application)**

Application that determines a possibly empty candidate list by collecting one or more biometric samples from a biometric capture subject and searching the enrolment database for similar biometric references.

**NOTE** Biometric references may be judged to be similar on the basis of comparison score.

3.5.10 **positive identification (deprecated)**

**NOTE 1** Use of this term is deprecated to avoid confusion between biometric verification (3.2.4.1.3) and biometric identification (3.2.4.1.2).

**NOTE 2** This term has been used in biometrics to mean biometric verification (3.5.4) of a positive claim as to the source of a biometric reference in the database.

**NOTE 3** Preferred expression would be a positive identity claim.

3.5.11 **fallback (deprecated)**

### 3.6 Performance

#### 3.6.1 **biometric failure to enrol**

Failure of the biometric system to store a usable biometric reference due to deficiencies in the biometric data during an enrolment application.

**NOTE** Deficiencies in the biometric data manifested as failure to capture, failure to extract biometric features usable for biometric reference generation, or failure to generate a usable biometric reference.

#### 3.6.2 **biometric failure to enrol rate**

Proportion of biometric enrolment sessions (that did not fail for non-biometric reasons), that resulted in a biometric failure to enrol.

**NOTE 1** Basing the denominator on the number of biometric enrolment sessions may result in a higher value than basing it on the number of biometric capture subjects.

**NOTE 2** The proportion denominator is the number of biometric enrolment sessions, excluding those sessions that failed to complete for non-biometric reasons.

#### 3.6.3 **biometric match trial (previously referred to as “genuine trial”)**

Set of comparisons of biometric samples and biometric references from the same biometric data subjects and the same biometric characteristics.

**NOTE** Biometric match trials do not fully model the case where a biometric capture subject is trying not to be recognized.

#### 3.6.4 **biometric non-match trial (previously referred to as “impostor trial”)**

Set of comparisons of biometric samples and biometric references from different biometric data subjects.

**NOTE 1** If a decision of “match” for a recognition biometric sample and a biometric reference from different biometric characteristics of the same biometric data subject is considered to be a false match then the biometric non-match trials would also include such comparisons.
NOTE 2  Biometric non-match trials do not fully model biometric impostor trials.

NOTE 3  A biometric non-match trial need not contain all possible comparisons of biometric samples and biometric references from different biometric capture subject characteristics.

Editor’s note: should “…decision of “match” for …” in note 1 be changed to “…comparison decision of “match” for…”?

3.6.5  closed set false-negative identification error rate

3.6.6  closed set identification error

3.6.6.1  closed set combination identification error

3.6.6.2  closed set false-negative identification error

3.6.6.3  false-positive identification error

3.6.7  closed set identification error trials

3.6.8  detection error trade-off (DET)

3.6.9  equal error rate

3.6.10  failure to acquire
either a failure to capture or a failure to extract biometric features usable for biometric comparison or biometric reference generation due to deficiencies in the biometric data

3.6.11  failure to acquire rate
proportion of the [biometric application] [attempts] (that did not fail for non-biometric reasons), that result in a failure to acquire

NOTE  The proportion denominator is the number of biometric enrolment [attempts], excluding those [attempts] that failed to complete for non-biometric reasons.

3.6.12  failure to acquire rate for enrolment
failure to acquire rate where the [biometric application] is enrolment
3.6.13
failure to capture
biometric capture process that does not result in the creation of a usable biometric sample due to deficiencies in the biometric data

3.6.14
failure to process

3.6.15
false accept / acceptance

3.6.16
false accept rate

3.6.17
false match
comparison decision of “match” for a recognition biometric sample and a biometric reference that are from different biometric capture subjects

NOTE It is recognized that this definition considers only the false match at the subject level at not at the characteristic level. Sometimes a comparison decision of “match” for a recognition biometric sample and a biometric reference from different biometric characteristics of the same biometric data subject is also considered to be a false match. For example, a “match” decision when comparing Galton ridges of different fingers of the same biometric data subject might be considered a false match, while a “match” decision for a mispronounced pass-phrase in text-dependent speaker recognition might be considered a correct match.

3.6.18
false match rate
proportion of the completed biometric non-match trials that result in a false match

NOTE 1 The value computed for the false match rate will depend on thresholds, and other parameters of the comparison process, and the protocol defining the biometric non-match trials. In particular, treatment of comparisons between:
   — identical twins;
   — completely different biometric characteristics of different individuals, such as face topography and Galton ridges;
   — different, but related biometric characteristics from the same individual, such as left and right hand topography;
will need proper consideration. See ISO 19795-1.

NOTE 2 “Completed” refers to the computational processes required to make a comparison decision, i.e. failures to decide are excluded.

3.6.19
false non-match
comparison decision of “non-match” for a recognition biometric sample and a biometric reference that are from the same biometric capture subject and of the same biometric characteristic

NOTE There may need to be consideration on how much mis-action on the part of the biometric capture subject is tolerated before the recognition biometric sample and the biometric reference are deemed to be of different biometric characteristics.

3.6.20
false non-match rate
proportion of the completed biometric match trials that result in a false non-match

NOTE 1 The value computed for the false non-match rate will depend on thresholds, and other parameters of the comparison process, and the protocol defining the biometric match trials.
NOTE 2 "Completed" refers to the computational processes required to make a comparison decision, i.e. failures to decide are excluded.

3.6.21 false reject / rejection

3.6.22 false reject rate

3.6.23 open set identification error

3.6.23.1 combination identification error

3.6.23.2 false-negative open set identification error

3.6.23.3 false-positive open set identification error

3.6.24 open set false-negative identification error rate

3.6.25 open set false-positive identification error rate

3.6.26 open set identification error trials (maled)

3.6.27 open set identification error trials (no maled)

3.6.28 receiver operation characteristics (ROC)
Annex A
(informative)

Other Terms

A.1 No mapping requirement

Words from the priority list of terms with no requirement to appear on a concept map:

BioAPI and CBEFF terms:

- Biometric Data Block (BDB)
- Biometric Information Record (BIR)
- Biometric type and subtype

ISO/IEC 7816-11:2003:

- Biometric Information Template (BIT) – This concept was introduced in ISO/IEC 7816-11: 2003, Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods.

A.2 Terms used in natural language unspecific to biometrics

The following words should be used with respect to their natural language definition.

A.2.1 applicant
an individual who applies for something

NOTE 1 Definition source: Oxford dictionary

NOTE 2 The dictionary definition has been modified from “person” to “individual” for consistency with [ISO/IEC 15944-1:2002 (3.47)]. [NZ: Editor’s note: Suggest adding the following clarification sentence to this note: “For biometrics purposes, applicants are “natural persons” not “legal persons”, see Person (A.2.6).”]

A.2.2 authenticate
to prove or show to be of undisputed origin or veracity; genuine

NOTE Definition source: Oxford dictionary

A.2.3 capture
record or express accurately in words or pictures; cause data to be stored in a computer

NOTE Definition source: Oxford dictionary
A.2.4  
**database**
collection of data organized according to a conceptual structure describing the characteristics of these data and the relationship among their corresponding entities, supporting one or more applications

NOTE  Definition source: ISO 2382 Part 17, term 17.01.01

A.2.5  
**individual**
of or for a particular person; single human being or item as distinct from a group

NOTE  Definition source: Oxford dictionary

A.2.6  
**Person**
an entity, i.e. natural or legal person, recognized by law as having legal rights and duties, able to make commitment(s), assume and fulfill resulting obligation(s), and able of being held legally accountable for its action(s)

NOTE 1  Synonyms for “legal person” include “artificial person”, “body corporate”, etc. depending on the terminology used in the competent jurisdictional domain.

NOTE 2  Person is capitalized to indicate that it is being used as formally defined in the standards and to differentiate it from day-to-day use.

NOTE 3  Minimum and common external constraints applicable to a business transaction often require one to differentiate among three common subtypes of Person, namely, “individual”, “organization” and “public administration”.

NOTE 4  Definition and notes (1-3) source: [ISO/IEC 15944-1:2002 (3.47)]. See 15944-1:2002 for additional definitions of entity and commitment.

A.2.7  
**registration**
the action or process of registering or of being registered; exact correspondence of the position of printed matter on the two sides of a leaf

NOTE 1  Register – v – enter in or place on a register.

NOTE 2  Register – n – an official list of record.

NOTE 3  Definition source for registration and register (verb and noun): Oxford dictionary.

A.2.8  
**score**
NOTE  Use in the natural language sense.

A.2.9  
**scoring**
NOTE  Use in the natural language sense.

A.2.10  
**subject**
NOTE 1  Use in the natural language sense.

NOTE 2  An individual undergoing a biometric process is typically referred to as a biometric subject, further qualified by the type of process. For example, biometric capture subject and biometric data subject. This helps clarify the different roles of individuals, such as attendants and biometric capture subjects.
A.2.11  
**system**  
an organized scheme or method; a complex whole; a set of things working together as a mechanism or interconnected network  

NOTE Definition source: Oxford dictionary

A.2.12  
**validation**  
process of checking or proving the validity  

NOTE 1 This is a particular definition from the Oxford dictionary which is most representative of the use of the term within biometrics.  

NOTE 2  Valid – adj – actually supporting the intended point or claim (Oxford dictionary)

A.2.13  
**verify**  
make sure or demonstrate that something is true, accurate or justified  

NOTE Definition source: Oxford dictionary.
Annex B
(informative)

Process flow diagram

<Recognition biometric sample>

Captured biometric sample

Intermediate biometric sample processing

Intermediate biometric sample

Feature extraction

Biometric feature

Training for model

Biometric model

Comparison

Comparison score

Qualification/thresholding/winnowing

Comparison decision

Threshold

Decision policy

Biometric application decision

accept claim/reject claim/special treatment

<Enrolment biometric sample>

Enrolment

Database or storage media (ex. IC card)

Biometric reference

Captured biometric sample

Intermediate biometric sample

Biometric template

Biometric model

[Auxiliary] biometric reference (new)

Universal background model, mean face, etc...

Proposed diagram for UK meeting by JNB
Annex C
(informative)

Concept diagrams

C.1 Graphic representations used in the concept diagrams

**Generic relations**
- are represented by tree diagrams

**Partitive relations**
- are represented by rake diagrams

**Associative relations**
- are represented by arrow diagrams

**Concept relations which are not explicitly shown in the definitions**
- are represented by dashed lines

**Multidimensional subdivision: criterions of subdivisions**
- are represented by thicker lines

Entry items are shown in boldface; terms referring to concepts which are not defined in the vocabulary are given in parenthesis
C.2 Biometrics sub-field delimitation

Note: We must go through the preliminary designations in a consistent manner regarding the qualifier “biometric …” in accordance with the following principle decided upon in New Zealand:

- If there is another definition for a word/term that strongly conflicts with our use of the word, we should use the “biometric” qualifier.
C.3 General concepts

C.3.1 General concepts 1

- **CN:** General concepts (sub-field)
  - Superordinate concept
  - Biometric types, modality [M] (essential)
  - Related to all sub-field [M]
  - Anything that related to all aspects of biometrics
  - Familiar to the general public
  - Superordinate sub-field in whole sub-fields (essential)
  - Plus more to be determined
- **PD:** General concepts

- **CN:** Biometric algorithm
  - block or sub-block of computer code in a biometric system that processes biometric data
- **PD:** Biometric algorithm

Examples: Signal detection, segmentation, biometric feature extraction, quality assessment, biometric model generation, biometric template generation, comparison, decision, compression, decompression, etc.

Note this is not an exhaustive list of general concepts.

- **CN:** Biometric (adj)
  - Of or having to do with biometrics
- **PD:** Biometric

Proposed defn: of or having to do with biometrics

**NOTE**
- The use of biometric as a noun, to mean for example, biometric characteristic, is deprecated.

**EXAMPLE** Incorrect usage #1: ICAO resolved that face is the biometric most suited to the practicalities of travel documents.

**EXAMPLE** Correct usage #1: ICAO resolved that face recognition is the biometric modality most suited to the practicalities of travel documents.

**EXAMPLE** Incorrect usage #2: The biometric recorded in my passport is a facial image.

**EXAMPLE** Correct usage #2: The biometric characteristic recorded in my passport is a facial image.

- **CN:** Biometric Mode (noun), Modal (adj)
  - Combination of a biometric characteristic, a biometric capture device type or subtypes and a method of processing

Proposed def: combination of a biometric characteristic, a biometric capture device type or subtypes and a method of processing

See next page.

- **CN:** List of currently used biometric characteristics:
  - Face
  - Fingerprint
  - Iris
  - Voice
  - Vein
  - Hand geometry
  - DNA
  - Signature
  - Palm print

- **CD:** List of sensor types:
  - For example:
    - Optical
    - Infrared
    - Acoustic

Sensor Subtypes:
- 2D optical
- 3D optical

- **CN:** List of processing methods:
  - For example:
    - Spectral decomposition (PCA, Mel-CC)
    - Correlation (Texture)
    - Graph matching

See JP comment on "mode" on next page!
C.3.2 General concepts 2

CN: biometric modality
- Dependent on biometric characteristic
- Requires a processing stream
- Human perception mechanism may distinguish modalities
- Biometric modality may depend on sensor type – only if we are talking about interaction of different physical properties
- Measurement bands, or number of them being used will determine if something is single or multimodal
- Can be used for the purpose of automated recognition of individuals
- From which distinguishing, repeatable features can be extracted
- Attributes of an individual’s biology and behaviour
- Observable
- Morphologically related physical properties…

WG2:
- Only difference between characteristic and modality is its use in a biometric system
- Processing stream
- Biometric process that involves fusion and more than one biometric characteristic/trait
- Quick notes taken while Rick speaking:
  - Modality – uses a single characteristic and separates it out into a separate process
  - Needs to include multiple characteristics through multiple processing streams
  - Multiple characteristics through a single processing stream is single modality.
  - RGB channel – treat each channel separately – multisensor, not multimodal
  - Multisensor includes different sensor types
  - Smart Gate: Simages of the face taken at once. Compared sequentially for a match – multi-presentation

- If physical property is different
- Different band may sense a different body part
- Processing path

PD: biometric modality

History:
Biometric modality is determined by the biological and behavioural characteristics, the method of observation and the method of feature extraction.
This does not imply that “each” unique combination is a “different” modality.

Galton ridge structure + sensor A + spectral decomposition = single modality [1]
Galton ridge structure + sensor A + minutiae = single modality [but equal to 1?]
Should biometric modality = biometric characteristic

Modality – (Oxford) modal quality; a method or procedure; a form of sensory perception
Modal – (Oxford) of or relating to mode or form as opposed to substance
Mode – (Oxford) a way in which something occurs or is done

Come back to this

London:
JP.2: The difference between “biometric type (subtype)” and biometric modality (3.2.2.2.6) is ambiguous.
WG1 should harmonize them because they have already used in both 19784 and 19785 as a synonym of biometric characteristic (3.2.2.2.1). Suggestion: Both “biometric type” and “biometric subtype” should be used as elements of biometric characteristic (3.2.2.2.1), ex, fingerprint, iris, face, etc…
Final thoughts in London: maybe we need to deprecate use of this concept!!!
C.3.3 General concepts 3 (for history purposes when discussing biometric modality again)

History:
CN: biometric characteristic (trait, attribute)
- From which distinguishing, repeatable features can be extracted
- Attributes of an individual’s biology and behaviour
- Observable
- Biological and behavioural characteristics = Body parts, substructures of body parts, physiological and behavioural processes created by the body and combinations of any of these
- Dialectic constant
- Physical property
- Sensible property
A sensible property of

Keep all these for historical reasons in corpus, but these are deleted from the concept map:
- Defin for body part – macrostructure
- Don’t like measurable as it implies extraction
- Body / bodily movements
- Characteristics can be embedded in other characteristics
- Always appear in multiple
- Properties to be measured of the individual
- Biological features
- Correction – biometric characteristic does not have to be distinguishing, but the relationship
- Cannot be a biometric char unless there is distinguishing capabilities
- Distinguishing – not all people have it in that
- To be used for recognition
- Characteristic may contain both distinguishing and non-distinguishing information
- Distinguishing is a property of the algorithm, not the characteristic!!

PD: biometric characteristic
Proposed defn:
biometric (deprecated)
biological and behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals

NOTE 1 Biological and behavioural characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these.

NOTE 2 Distinguishing does not necessarily imply individualization.

EXAMPLE Examples of biometric characteristics are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, etc.

JP-3 comment:
Add the NOTE or EXAMPLE about:
- whole face and parts
- the face under visible light and infrared light
- minutia and pattern
to define biometric characteristics.

Oxford: Observe – notice; perceive; watch; detect in the course of scientific study
Transducer – a device that converts variations from a physical quantity such as pressure or brightness into an electrical signal. <If you have an optical signal system, this would not apply>

John’s comment:
Added with "and behaviour" changed to "or behaviour"
Surely "biology" is wrong? Is a fingerprint a trait of an individual's biology? What is trait anyway? This is a weak definition.

This information is left here for use in discussing biometric modality concept
C.4 Biometric system

C.4.1 Biometric system components

CN: System
PD: System
Oxford defn: An organized scheme or method; a complex whole; a set of things working together as a mechanism or interconnected network

CN: Biometric system
PD: biometric system
Proposed defn: system for the purpose of the automated recognition of individuals based on their behavioural and biological characteristics

CN: Verification system
PD: biometric verification system
Proposed defn: system which performs biometric verification

CN: Biometric product
PD: biometric product
Proposed defn: biometric article in the form of equipment or implemented software which has been manufactured or refined for sale

Oxford:
Product: Article or substance manufactured or refined for sale
History:
Statements out there:
• anything which is produced is a product
• Should instead reserve the word “product” for something that can be bought.
• Happy to use product in dictionary sense and biometric in adjective sense.
• Term is used in 19792
Berlin Note: check definition with BioAPI and CBEFF
C.5 Data in biometric systems

**CN: Enrolment data record**
- May be empty
- Includes:
  - Non-biometric data associated with a biometric data subject, a biometric sample, or a biometric reference
  - Biometric reference(s)
- Need not be the only record for that biometric data subject

**PD: enrolment data record**
Proposed defn: record created upon enrolment, associated with the biometric data subject and including biometric reference(s) and typically non-biometric data

**CN: Enrolment database**
- The part of the biometric system database linking enrolled biometric references to Biometric Reference identifiers
- Database can be on any storage medium and can be of any size (including a single entry)

**PD: biometric enrolment database**

---

**Sub-sub-field: Biometric data terms**

**Sub-sub-field: Non-biometric data**

---

**Overlapping concepts**

- CN: Enrolment database
- Record (from ISO 2382 Part 17, term 17.05.12)
- Data object (from ISO 2382 Part 17, term 17.01.11)

**CN Concept name**
- Essential characteristic

**PD Preliminary designation**
- Characteristics developed by WG1
- Characteristics need further development by WG1
- Associative relation

---

**London:**
RF.5: Consider all definitions which use “enrolment database/biometric enrolment database” and decide which one of “database” or “biometric enrolment database” to use in each case
C.5.1 Figure to be used during discussions of biometric sample and biometric data related terms

Editor’s Note: Get updated diagram from SD11 harmonization document update
## C.5.2 Biometric data terms

### C.5.2.1 Biometric data terms 1

<table>
<thead>
<tr>
<th>CN: Biometric sample</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>• Representation of biometric characteristics between the capture process and the feature extraction process</em></td>
</tr>
<tr>
<td><em>• Analog or digital</em></td>
</tr>
<tr>
<td><em>• Regardless of how it was taken from a subject or capture medium with a biometric capture device</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PD: Biometric sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed defn: analog or digital representation of biometric characteristics prior to biometric feature extraction process and obtained from a biometric capture device or biometric capture subsystem</td>
</tr>
<tr>
<td>NOTE: A biometric capture device is a biometric capture subsystem with a single component</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: Captured biometric sample</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>• Biometric sample</em></td>
</tr>
<tr>
<td><em>• Output of biometric capture device</em></td>
</tr>
<tr>
<td><em>• Representation of biometric characteristics for further processing</em></td>
</tr>
<tr>
<td><em>• Analog or digital</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PD: Captured biometric sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed defn: raw biometric sample (deprecated)</td>
</tr>
<tr>
<td>biometric sample that is output of biometric capture process</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History:</th>
</tr>
</thead>
<tbody>
<tr>
<td>captured was chosen over acquired here to preserve the commonly used term failure to acquire – however, we may want to consider deprecating the term failure to acquire – jury is still out</td>
</tr>
<tr>
<td>Defn changed from “biometric sample that is input to intermediate biometric sample processing” in Berlin</td>
</tr>
</tbody>
</table>

| London: JP.6: In SD2v5, “acquire biometric sample” is disappeared. Other editors have already referred SD2v4 and incorporate the acquired biometric sample into their documents. To avoid confusion, WG1 should add “acquired biometric sample” as a deprecated index term and NOTE that “acquired” has been changed to “captured” with appropriate reason. Suggestion: Add acquired biometric sample (deprecated) and NOTE(reason). |
| Disposition: Agree, but make decision once we have decided what to do with failure to acquire |

| Berlin: JP10 C.4.2.1 The definition of failure-to-acquire in C.7.6 resolved the comment JP1 for CN: captured biometric sample. New comment on the distinction between captured biometric sample and acquired biometric sample should be added in the NOTE. Suggest: Delete JP6 comment for CN: captured biometric sample, and add NOTE: acquired biometric sample successfully processed by acquire process including such as feature extraction is distinct from captured biometric sample. |
| Disposition: Rejected as comment but will be considered during discussion of concept maps covering acquire process |

<table>
<thead>
<tr>
<th>CN: Biometric reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>• Stored</em></td>
</tr>
<tr>
<td><em>• One or more templates, models or biometric samples</em></td>
</tr>
<tr>
<td><em>• Attributed to an individual at enrollment</em></td>
</tr>
<tr>
<td><em>• Used for comparison</em></td>
</tr>
<tr>
<td><em>• Examples: Face image on a passport; Minutiae template on a National ID card; Gaussian Mixture Model in a database.</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PD: Biometric reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed defn: one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison</td>
</tr>
<tr>
<td>EXAMPLE Face image on a passport; Fingerprint minutiae template on a National ID card; Gaussian Mixture Model, for speaker recognition, in a database.</td>
</tr>
<tr>
<td>NOTE A biometric reference may be created with implicit or explicit use of auxiliary data, such as Universal Background Models.</td>
</tr>
</tbody>
</table>

| ***To consider – reference may include cohort information*** |
| Consider adding additional NOTE to defn to state: a reference attributed to an individual may include pointers to information from other individuals |

<table>
<thead>
<tr>
<th>History:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unless someone can think of a recognition model, then we do not need to create a symmetric word for reference in the recognition space.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: Biometric template</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>• Stored Biometric features</em></td>
</tr>
<tr>
<td><em>• Attributed to an individual at enrollment</em></td>
</tr>
<tr>
<td><em>• Type of biometric reference</em></td>
</tr>
<tr>
<td><em>• Comparison uses a function not dependent on individual e.g., Hamming distance, Euclidean distance, etc., although it’s parameters might be directly compared to sample features</em></td>
</tr>
<tr>
<td><em>• Set of features that can be compared directly to the input features to give a score</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PD: Biometric template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed defn: set of stored biometric features comparable directly to biometric features of a recognition biometric sample</td>
</tr>
<tr>
<td>NOTE 1 A biometric reference consisting of an image, or other captured biometric sample, in its original, enhanced or compressed form, is not a biometric template.</td>
</tr>
<tr>
<td>NOTE 2 The biometric features are not considered to be a biometric template unless they are stored for reference.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: Intermediate biometric sample</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>• Processed captured biometric sample prior to feature extraction</em></td>
</tr>
<tr>
<td><em>• (Enhanced) for feature extraction</em></td>
</tr>
<tr>
<td><em>• (Enhanced) for storage or transmission</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PD: Intermediate biometric sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed defn: biometric sample that is output of intermediate biometric sample processing</td>
</tr>
<tr>
<td>EXAMPLE Intermediate biometric samples may have been enhanced for biometric feature extraction, compressed for compact storage purposes, etc.</td>
</tr>
</tbody>
</table>
C.5.2.2 Biometric data terms 2

CN: Biometric model
- Stored Function (dependent on the biometric data subject) generated from enrollment biometric features
- Function may involve training aspect
- Attributed to a biometric data subject at enrollment
- Type of biometric reference
- Comparison applies the function to the sample features to give a score

PD: Biometric model
Proposed defn: stored function (dependent on the biometric data subject) generated from biometric feature(s)

NOTE 1 Comparison applies the function to the biometric features of a recognition biometric sample to give a comparison score.
NOTE 2 The function may be determined through training.
NOTE 3 A biometric model may involve intermediate processing similar to biometric feature extraction.

EXAMPLE Examples for the stored function could be a Hidden Markov Model, Gaussian Mixture Model or an Artificial Neural Network.

CN: Biometric feature
- output of a completed biometric feature extraction process
- numbers or labels extracted from biometric samples and used for comparison

PD: Biometric feature
Proposed defn: numbers or labels extracted from biometric samples and used for comparison

NOTE 1 Biometric features are the output of a completed biometric feature extraction process.
NOTE 2 The use of this term should be consistent with its use by the pattern recognition and mathematics communities.
NOTE 3 A biometric feature set can also be considered a processed biometric sample.

History: Definition changed from “output of a completed biometric feature extraction process” at Berlin meeting. Also, prior Note 2: “An uncompleted biometric feature extraction process might be an error message or a NULL vector.” deleted.

Need generic term for biometric sample / biometric feature / biometric model

Pointer from Biometric template and Biometric reference
C.5.2.3 Biometric data terms 3

CN: Probe

- Unsettled claim has been made about this data
- As opposed to reference
- To be compared to the reference
- Could consist of unlabeled:
  - biometric samples
  - biometric features

Notes:
- Query (adj) is possibly used in the pattern recognition community
- 2382-17: 17.07.08 query (n) a request to extract data directly or to derive them from a database based on specified conditions
- Japan suggest to use probe only as adjective
- Probe as a noun is difficult in Russia
- Tried and deleted:
  - Test – confusing between testing and operational systems
  - Checking – confusion with comparison
  - Sample – don’t want sample biometric samples
  - Input – then you would be inputting the reference and the input
  - Acquired – already being used – unless we re-write acquired biometric sample; also confusion with failure to acquire

PD: recognition

Other suggested PDs: recognition / claim / query / submitted / quest

- LONDON: JP.9 “Probe” should be deprecated. Suggest recognition. Probe (deprecated).
- Need to define recognition biometric samples, features and models

NZ: revisit use of “biometric recognition” as preferred term in “Authentication” term in main body

Berlin: German comment: DE 9 on term 3.2.4.1.5: “recognition biometric sample” is hard to read out.
- Suggest: Change to “process in which a biometric recognition sample …” here and elsewhere in the document. Disposition of comment: revisit words when issue of ‘recognition’ is settled

CN: Biometric property / individuality

- Attributes of the biometric data subject estimated or derived from the biometric sample

PD: Biometric property

Proposed defn: descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means

EXAMPLE: Fingerprints can be classified by the biometric properties of ridge-flow, i.e. arch, whorl, and loop types; In the case of facial recognition, this could be estimates of age or gender.

CN: biometric data for recognition

recognition biometric sample
(recognition ) biometric model
(recognition ) biometric feature
PD: recognition biometric data

CN: recognition (adjective)

adjective when it used for recognition
PD: recognition

Berlin:
- German comment: DE 9 on term 3.2.4.1.5: “recognition biometric sample” is hard to read out. Suggest: Change to “process in which a biometric recognition sample …” here and elsewhere in the document. Disposition of comment: revisit words when issue of ‘recognition’ is settled

CN: biometric data

- biometric sample at any stage of processing
- biometric reference
- biometric feature
- biometric property
- (need to consider if other data can be considered biometric data – such as Universal Background Models, etc.)

Berlin: Is biometric data both population data not attributable to any specific individual (UBM, eigenface) and data attributable to a specific individual?

PD: biometric data

CN: reference maturity

- Reference template
- Ageing
- Maturity
PD: reference maturity

Where does this go?

CN: biometric data for recognition

recognition biometric sample
(recognition ) biometric model
(recognition ) biometric feature
PD: recognition biometric data

CN: recognition (adjective)

adjective when it used for recognition
PD: recognition

Berlin:
C.5.2.4 Biometric data terms 4

<table>
<thead>
<tr>
<th>To which concept map does this belong?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN: biometric characteristic (trait, attribute)</td>
</tr>
<tr>
<td>- From which distinguishing, repeatable features can be extracted</td>
</tr>
<tr>
<td>- Attributes of an individual’s biology and behaviour</td>
</tr>
<tr>
<td>- Observable / detectable</td>
</tr>
<tr>
<td>- for the purpose of automated recognition of individuals</td>
</tr>
<tr>
<td>- Biological and behavioural characteristics = physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PD: biometric characteristic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed defn: biometric (deprecated)</td>
</tr>
<tr>
<td>biological and behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals</td>
</tr>
<tr>
<td>NOTE 1 Biological and behavioural characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these.</td>
</tr>
<tr>
<td>NOTE 2 Distinguishing does not necessarily imply individualization.</td>
</tr>
<tr>
<td>EXAMPLE Examples of biometric characteristics are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, etc.</td>
</tr>
</tbody>
</table>

Examples of biometric characteristics are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, <the way one writes a signature (signature?)>, <the way one speaks (voice?)>, <the way one types (keystroke?)>.

History:
Note: Biometrics will use the characteristics for which we have algorithms extracting distinguishing features.
C.5.3 Non-biometric data

Sub-sub-field: Non-biometric data produced in biometric processing

Sub-sub-field: Non-biometric data associated with administration

Sub-sub-field: Non-biometric data associated with a biometric data subject, a biometric sample or a biometric reference

Privacy and biometric data not associated with a Person

Editor’s suggestion: Placed this here because of placement of the inserted slide on this topic as output from meeting in Berlin. However, given the title, I recommend splitting “sub-sub-field: Biometric data terms” into 2:
- sub-sub-sub-field: Biometric data terms associated with a Person
- sub-sub-sub-field: Biometric data terms not associated with a Person

CN: Non-biometric data
PD: Non-biometric data
Proposed defn: any data associated with biometric data which is not derived from biometric samples
Editor’s note: Where should this be added in main body?
Editor’s note: Do we consider UBM biometric or non-biometric data?
Berlin: data associated with a biometric data:
  • not derived from biometric samples
  • Population or individual level data
C.5.3.1 Non-biometric data produced in biometric processing

C.5.3.1.1 Non-biometric data produced in biometric processing 1

**CN: Biometric reference identifier**
- A pointer to a biometric reference in the enrolment database

**PD: Biometric reference identifier**
Proposed defn: pointer to a biometric reference in the enrolment database

**CN: Candidate**
- Degree of certainty above some score threshold
- Not necessarily the final decision
- A Biometric Reference identifier in the enrolment database that resembles the input biometric sample according to "comparison" criteria
- The selection might be on the basis of comparison score or rank

**PD: Candidate**
Proposed defn: biometric reference identifier in the enrolment database determined to be similar to the recognition biometric sample
NOTE Determination may be on the basis of comparison score and/or rank.

**CN: Candidate list**
- Set of zero, one or more Biometric Reference identifiers in the enrolment database that resemble the input biometric sample according to selection criteria
- May be tentative if to be reduced by further process

**PD: Candidate list**
Proposed defn: set of zero, one or more candidates that may be intermediate or final
NOTE Intermediate candidate lists may be produced by systems that use multi-pass biometric identification

**CN: Candidate score**
- A numerical value (or set of values)
- Result of comparison of an input biometric sample and biometric reference indicating the degree of similarity

**PD: Candidate score**
Proposed defn: comparison score for a candidate
NOTE Higher is not meant to mean more similar.

**CN: Comparison score**
- A numerical value (or set of values)
- Result of comparison of an input biometric sample and biometric reference indicating the degree of similarity

**PD: Comparison score**
Proposed defn: matching score (deprecated) numerical value (or set of values) resulting from a comparison
NOTE Higher is not meant to mean more similar.

**CN: Comparison decision**
- Based on (1) comparison score; (2) decision policy including threshold, and other inputs needed by decision policy;
- Possible values: Match / Non-match / possible other values such as "undetermined" in accordance with decision policy
- A determination of whether or not the recognition biometric sample and biometric reference have the same biometric source.

**PD: Comparison decision**
Proposed defn: determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies) including a threshold, and possibly other inputs.
NOTE 1 A match is a positive comparison decision.
NOTE 2 A non-match is a negative comparison decision.
NOTE 3 A decision of "undetermined" may sometimes be given.

**CN: Similarity score**
- Comparison score that increases with similarity

**PD: Similarity score**
Proposed defn: comparison score that increases with similarity

**CN: Dissimilarity score**
- Comparison score that decreases with similarity

**PD: Distance score/Dissimilarity score**
Proposed defn: comparison score that decreases with similarity
C.5.3.1.2 Non-biometric data produced in biometric processing 2

**CN: Match (noun)**
- Decision, based on a decision policy
- Applies to both identification and verification attempts
- Input:
  - Biometric reference
  - Recognition biometric sample / feature / model
- Output:
  - Decision that the sample and the reference are from the same source

**PD: match**
Proposed defn: comparison decision that the recognition biometric sample(s) and the biometric reference are from the same source

*Oxford:* a person or thing that resembles or corresponds to another

*History:* alternative suggested definition biometric recognition result stating that the recognition biometric sample(s) and the biometric reference show a specified degree of similarity

**CN: Comparison decision**
- Based on (1) comparison score; (2) decision policy including threshold, and other inputs needed by decision policy
- Possible values: Match / Non-match / possible other values such as "undetermined" in accordance with decision policy
- A determination of whether or not the recognition biometric sample and biometric reference have the same biometric source.

**PD: Comparison decision**
Proposed defn: determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies) including a threshold, and possibly other inputs

*NOTE 1* A match is a positive comparison decision.
*NOTE 2* A non-match is a negative comparison decision.
*NOTE 3* A decision of "undetermined" may sometimes be given.

**CN: No-Match**
- Not a match

**PD: non-match**
Proposed defn: comparison decision that the recognition biometric sample(s) and the biometric reference are not from the same source

*History:* alternative proposed definition: biometric verification result stating that the recognition biometric sample(s) and the biometric reference do not show a specified degree of similarity
C.5.3.2 Non-biometric data associated with a biometric data subject, a biometric sample or a biometric reference

**CN: Claimed identity**
- Reference in a biometric enrolment database
- Assertion about source of biometric reference

**PD:**
Proposed defn: reference in a biometric enrolment database to which an assertion is made that a biometric capture subject is the source

**NOTE** Usually made in the first person

**CN: Individual metadata**
- E.g. Access privileges, authorizations, name, address
- Information that is not derived from biometric characteristics
- Data specific to a person (as opposed to specific to a body)
- Person and legal person
- Information may become outdated
- Linked to biometric data or null biometric data record

**PD:**
Proposed Defn: non-biometric data associated with the data subject but independent of the capture of the biometric sample e.g. name, address, gender, marital status

**Berlin Note:** In some cases of legal guardianship the person to whom the metadata refers may not be the person who supplied the biometric sample

**CN: Biometric sample metadata**
- Examples
  - Timestamp, ...
  - E.g. left or right eye
  - Machine used for collection
- Relevant to and associated with sample
- Taken when the biometric data sample is captured or processed
- May or may not be derived from the sample itself
- Not descriptive or representative of biometric data subject
- Descriptive information regarding the associated biometric data
- Always remains true after the data collection
- Excludes data logs

**PD: Biometric sample metadata**
Proposed Defn: non-biometric data associated with the capture and processing of the biometric sample but independent of the data subject e.g. timestamp, collection device, modality

**Berlin Note:** some aspects of the metadata such as camera resolution or modality may be verifiable from the biometric data itself

**London:** DE.11/12 Consider including a note with this definition that indicates this may be synonymous with Biometric Information Template from 7816-11 (included in A.10)

**Berlin Note:** We have checked the SC17 7816-11 document and decided that it is not synonymous

**CN: Ground truth**
- The collection of measurement data by means other than the measuring instrument itself that is normally used, in order to validate the instrument is sufficiently accurate at reporting its results. It is a term which is used a lot in geology. The intention with biometrics is probably more to check the extrapolation of data.
- Validation of statistical extrapolation of information through spot checks (AUS proposal – not accepted as defn – needs work)

**PD:**

**Berlin Note:** this needed at all? Term is not specific to biometrics. Check with termium whether this or a similar word is already defined

**CN: Biometric data log**
- Example: access log
- Relevant to and associated with sample
- Not taken when the biometric data sample is captured
- Not derived from the sample itself
- Not descriptive or representative of biometric data subject
- Descriptive information regarding the history of the associated biometric data and its use

**PD: Biometric data log**
Proposed Defn: non-biometric data associated with the history and use of the biometric sample

**Berlin Note:** this term is differentiated from biometric sample metadata which remains static
C.5.3.3 Non-biometric data associated with administration

**Sub-sub-sub-sub-field:** Decision policy

**CN:** Decision policy
- Rules for making biometric application decisions
- Not dependent on an input biometric sample
- Could reflect current security level or purpose to which a decision will be put

**PD:**
*Proposed defn:* rules, principles or procedures by which biometric application decisions are made

Biometric application decision: conclusion based on the application decision policy after consideration of one or more comparison decisions, comparison scores and possibly other non-biometric data.

**NOTE 1** Biometric application decisions can be made on the basis of complex policies, allowing for variable numbers of positive comparison decisions.

**NOTE 2** A biometric verification (3.5.4) application could allow a positive biometric application decision even if there are one or more non-matches against enrolled biometric references.

**EXAMPLE** A biometric application decision could be "accept claim".

**Oxford defn of Policy**
Course or principle of action adopted or proposed by an organisation or individual

**Sub-sub-sub-sub-field:** Signal processing parameters and environment conditions

**CN:** Threshold
- A parameter for the biometric system against which a score of any type is compared
- Decision boundary
  - Match / Non-match
  - Adequate/inadequate quality
  - Pre-selected / or not
  - Candidate identifier or not

**PD:**
*threshold*
Oxford: A level or point at which something would start or cease to happen or come into effect

**CN:** rejection
- Verification transaction
- The system’s decision process fails to confirm the claim of identity
- NOTE: Includes failure to acquire adequate features

**PD:**
*Berlin Note:* what about enrollment transactions? If the word rejection cannot be used then we will need a new word covering enrollment transactions

**CN:** data capture conditions
- Illumination
- Noise
- May or may not be part of the biometric system
- Could apply to non-biometric data
- May impact the behaviour of the subject
- May impact the capture medium

**PD:**
*data capture conditions*
Berlin: Also appears on CM Data Capture Family 1
C.5.3.4  Privacy and biometric data not associated with a Person

**CN: Aggregated Biometric Data**
- universal background model, eigenfaces
- Aggregated data
- Comes from real individuals
- refer to biometric reference definition note.
- Biometric data not attributable to any individual

**PD: Aggregated biometric data**
Proposed defn: biometric data aggregated or averaged for a population and not associated with any single individual. Examples include, Universal background models and eigenfaces

**CN: Anonymous biometric data**
- Not associated with an individuals metadata
- Capable of being connected with existing individual metadata by non-biometric processing e.g. database keys and lookups
- Not anonymous for holder of keys

**PD: Anonymous biometric data**
Proposed defn: biometric data not currently associated or linked with any single individual. Examples include, finger marks or latents

**Berlin Note:** The anonymised biometric data cannot only be re-associated with the individual metadata by the holder of the data

**CN: Individualisable Anonymous biometric data**
Can be associated with individual metadata through biometric processing providing individual metadata exists

**PD:**
Proposed Defn. Biometric data not currently linked with any single individual metadata record but capable of being linked through biometric means

**Berlin Note:** Metadata may not exist

**CN: Non-individualisable Anonymous biometric data**
- Not capable of being associated with an individuals metadata through any current means
- Can be considered as non-biometric data

**PD:**
Proposed defn: Data not currently linked to an individual metadata record, nor capable of being linked through any means

**Berlin Note:** this is not usable Biometric data
C.6 Devices

C.6.1 Devices 1

CN: Biometric capture/input device / biometric sensor

- Hardware
  - Output an analog or digital signal
  - Has a transfer function – alters the signal in some way
  - Could be the capture medium or could interface with the capture medium
  - Capture medium could be part of the biometric device, but need not be
  - Part of the biometric system
  - Must have a direct interface to send the signal on for further processing
  - Capability to acquire a sample usable (potentially can result in the extraction of biometric features) for biometric processing
  - Transduces a signal from, or off of, the biometric characteristic (face – transduces optical wavelength light into an electrical signal, hand geometry – infrared light into an electrical signal; fingerprinting – frustrated total internal reflection: transduces the light off an infrared LED into an electric signal)
  - Signal is converted into a biometric sample
  - An illumination source is interacting with the biometric characteristic and the device is
  - Creates a decision point at which a decision could be made as to whether to accept the image into the biometric system

PD: biometric capture device

Oxford: Device: A thing made or adapted for a particular purpose; a plan, a scheme, a trick

Proposed defn: device that collects a signal from a biometric characteristic and converts it to a captured biometric sample

NOTE 1 A signal can be generated by the biometric characteristic or generated elsewhere and affected by the biometric characteristic, for example, face illuminated by incident light.

NOTE 2 A device can be any piece of hardware (and supporting software and firmware).

NOTE 3 A biometric capture device may comprise components such as an illumination source, one or more biometric sensors, etc.

History:
Kyoto: the last stage whereby what comes after that is what the computer uses (changed in London with introduction of biometric capture process)

Note: direct interface does not imply instantaneous transmission to the rest of the biometric system

Note: excludes digital cameras used without direct interface, but a digital camera is frequently used as a capture medium

Then failure to capture would imply that at this decision point a signal was judged to be not usable.

Failure to acquire in 19795-1, means biometric features could not be created. Thus failure to acquire actually must look at both a potential failure to capture and a failure to process.

Failure to enrol could include a proper extraction of features, but they were considered unstable

Discussion – restrict biometric capture device only to device that accept a signal from an individual directly into a biometric system. Thus a digital photo taken outside the biometric system, and later added to the biometric system, the camera is not a biometric capture device.

2 devices needed perhaps: a reference capture device and a recognition capture device

Active / passive device?

Note: quality (and resolution) of the output of the biometric capture device is dependent on all components within the capture process
C.6.2 Devices 2

CN: Capture tool
- Recording tool which records biometric characteristics in a certain media.
- Transducer which transfers captured data to other communication channel.
- Sensor may be included. Captured data is not always used as "biometric data", e.g. image data taken by digital camera is not biometric data but just raw data.

Example:
- IC card
- Compact flash etc.
- Glass
- Camera
- Ink and paper for fingerprint
- Handset for speaker recognition
- Tape recorder, IC recorder

PD:

CN: Direct capture device
- Device for capturing biometric sample from biometric characteristic directly and converting into electrical or digital data.
- Example: CCD camera which directly input capturing image into biometric system

PD:

CN: Indirect capture device
- Device for capturing biometric sample not directly from biometric characteristic but other media or channel.
- Build captured biometric sample.
- Example: IC card reader, Image scanner for photo, sound capture board for speaker recognition.

PD:

CN: Processing device
- To be developed, moved or removed.

PD:

CN: Intermediate media transformations
- PD: ???

CN: Capture medium
- The medium onto which a representation of the individual’s biological and behavioural characteristics were first recorded or captured.

PD: Capture medium

Note: for SC37 purposes we are only concerned with representations of an individual’s biological and behavioural characteristics.

Oxford:
medium: substance through which sensor impression are conveyed or physical forces are transmitted; a particular form of storage material for computer files such as magnetic tapes or disks; the middle quality or state between two extremes.

Capture: record or express accurately in words or pictures.

Capture medium: 2 major examples:
- Film
- Astrophysics

Example: A glass is an example when a fingerprint has been left on it.

Berlin Note: low priority words, principally needed
For other definitions.
C.7 Functioning

- Sub-sub-field: Data management terms
- Sub-sub-field: Data capture family (May not belong here)
- Sub-sub-field: Enrolment family
- Sub-sub-field: Signal processing family
- Sub-sub-field: Comparison family
C.7.1 Comparison family

C.7.1.1 Comparison family 1

**CN: Comparison**
- A type of scoring
- Any functions for comparing and scoring
- Includes pre-selection as well as comparison score generation
  - Input:
    - Biometric sample(s) / biometric feature(s) / biometric model(s)
    - Biometric reference(s)
  - Output:
    - Comparison score(s)

**PD: biometric comparison**
Proposed defn: match / matching (n) (deprecated as a synonym for comparison)
   estimation, calculation or measurement of similarity or dissimilarity between recognition biometric sample(s) / biometric features / biometric models and biometric reference(s)

**NOTE 1** Compare (v) – estimate, measure or note the similarity or dissimilarity between.

**NOTE 2** Match (v) is deprecated as a synonym to compare (v).

**CN: qualification / thresholding / winnowing**
- Comparison against threshold(s)
  - Input:
    - Score(s) pertaining to a biometric sample, a biometric reference, or both
  - Output:
    - 0/1 decision to eliminate or not some or all of the biometric sample(s), the biometric reference(s), or the pair(s)
    - Updated candidate list when appropriate

**PD: thresholding / cull / exclude**
Proposed defn: elimination of biometric reference identifier(s) associated with biometric reference(s) and/or identifiers for recognition biometric sample(s) that have failed to attain a level of any type of score

**NOTE** Score can be quality score, comparison score, etc.

**ARCHIVED**
CN: accept claim/reject claim/special treatment (was definitive decision)
- Biometric application decision output
  - One of accepting claim, rejecting claim or special treatment

**PD:**
NZ: Intent is to delete, but we want it here for discussion purposes.

**CN: Decision without an identifier/claim**
They may result in correct answer or incorrect answer

**PD:**
Berlin: Intent is to delete, but we want it here for discussion purposes. (E.g. IRIS entry or over 21 verification)

**CN: Decision with an identifier/claim**

**PD:**
Berlin: Intent is to delete, but we want it here for discussion purposes.

Do we need a decision subfield?

---

**Characteristics developed by WG1**

**Characteristics need further development by WG1**

**CN**
- Concept name

**PD**
- Preliminary designation
  - Essential characteristic
C.7.1.2 Comparison family 2

### CN: biometric identification (function call)
- **Preliminary designation**: biometric system function that performs a one-to-many comparison to obtain a candidate list
- **Proposed defn**: A biometric identification function may be used to verify a claim of enrolment in an enrolment database without a specified biometric reference identifier
- **Example**: BioAPI_IdentifyMatch
- **Note**: A biometric identification application (3.5.3) can use an exhaustive series of biometric verification function calls
- **Additional**: Re-address this concept in light of the change to one-to-many comparison to return only scores, not identifiers

### CN: biometric verification (function call)
- **Preliminary designation**: biometric system function that performs a one-to-one comparison
- **Proposed defn**: A biometric verification function call compares a recognition biometric sample/feature/model against a biometric reference to determine how likely it is that they are from the same source
- **Example**: BioAPI_VerifyMatch
- **Note**: Biometric verification comprises not only a one-to-many (or one-to-one) comparison resulting in a comparison score, but also a decision.
- **Suggestion**: Add at the end of the definition
- **NZ**: remove reference to one-to-one from definition

---

**CN**: Function
- **What is the ISO standard definition of function?**
- **PD**: biometric verification (biometric system function)
- **Proposed defn**: biometric system function that performs a one-to-many comparison to obtain a candidate list
- **Example**: BioAPI_IdentifyMatch
- **Note**: A biometric identification application (3.5.3) can use an exhaustive series of biometric verification function calls

**PD**: biometric verification (biometric system function)
- **Proposed defn**: biometric system function that performs a one-to-one comparison to obtain a candidate list
- **Example**: BioAPI_VerifyMatch
- **Note**: Biometric verification comprises not only a one-to-many (or one-to-one) comparison resulting in a comparison score, but also a decision.
- **Suggestion**: Add at the end of the definition
- **NZ**: remove reference to one-to-one from definition
C.7.1.3 Comparison family 3

**CN: One-to-one**
- Refers to the comparison process to produce a comparison score between one biometric data subject’s biometric sample (or samples within a single attempt)/features/model, and one biometric data subject’s biometric reference(s).
- **NOTE** An alternative viewpoint is that one-to-one should refer to comparison strictly between one biometric sample and one biometric reference (rather than the totality of comparisons to generate one sample-reference comparison score). In this case multimodal or likelihood ratio biometric verification would be considered one-to-many processes rather than a one-to-one comparison. Such a viewpoint would therefore violate common usage where “one-to-one” is given as a synonym for “verification”, and “one-to-many” a synonym for “identification”.

**PD: one-to-one comparison**
Proposed defn: process in which a recognition biometric sample / biometric feature / biometric model set from one biometric data subject is compared to biometric reference(s) to produce a comparison score with respect to one biometric data subject, perhaps using additional data from the enrolment database.

**NOTE 1** A biometric verification (3.2.4.1.3) function performs a one-to-one comparison.

**NOTE 2** In the case of a multimodal biometric system, the recognition biometric sample / biometric feature / biometric model and the biometric reference in the above definition comprise individual biometric samples / biometric feature / biometric model and biometric references of the component modalities.

**NOTE 3** A universal background model is not associated with a biometric data subject, therefore a comparison of a single biometric data subject’s sample to a claimed reference and a universal background model is not inherently one-to-many. In other words, use of a universal background model can still be one-to-one.

**CN: One-to-many / one-to-many search / one-to-many comparison**
- Refers to the comparison process to produce comparison scores between one biometric data subject’s biometric sample (or samples within a single attempt)/features/model, and many biometric data subject’s biometric reference(s).

**PD: one-to-many comparison**
Proposed defn: one-to-few (deprecated) process in which a recognition biometric sample / biometric feature / biometric model set of one biometric data subject is compared against the biometric references of more than one biometric data subject to return a set of comparison scores.

**NOTE 1** A biometric identification (3.2.4.1.2) function performs a one-to-many search.

**NOTE 2** In the case of a multimodal biometric system, the recognition biometric sample / biometric feature / biometric model and the biometric reference in the above definition comprise individual biometric samples / biometric feature / biometric model and biometric references of the component modalities.

**NOTE 3** A universal background model is not associated with a biometric data subject, therefore a comparison (3.2.4.6.2) of a single biometric data subject’s sample to a claimed reference and a universal background model is not inherently one-to-many.
C.7.2 Data management terms

CN: Loading biometric reference
- Transferring data between enrolment and comparison
- Retrieval from storage

PD: Berlin note: why is this term important?

CN: Deactivate
- Temporary removal of biometric data record search capability
- Proposed defn: Temporarily exclude biometric data reference(s) from biometric processing
- Berlin note: must be temporary to differentiate from de-enrolment

CN: Reactivate
- Make available deactivated biometric data record and references for biometric processing
- Proposed defn: reinstate previously deactivated biometric data references for biometric processing

PD: Berlin note: why is this term important?

History: In Berlin, De-enrolment moved to Enrolment concept map. Disaster recovery, Data updating, and Writing to storage concepts removed due to being general terms and outside of WG1 remit.
C.7.3 Data capture family

C.7.3.1 Data capture family 1 (may or may not be part of the biometric system)

- **CN: subject interface**
  - Gap between the individual and capture medium

- **CN: last point of transduction**
  - PD: ???

- **CN: presentation**
  - Facial expression
  - Rotation of finger
  - Pressure
  - Examples are PE from PIE (pose illumination expression)
  - Subject’s relationship to capture medium

- **CN: frontal presentation**
  - PD: ???

- **CN: right side presentation**
  - PD: ???

- **CN: left side presentation**
  - PD: ???

- **CN: [Physical factors] that impact data capture conditions**
  - Examples:
    - Illuminators and pegs for the hand
    - May or may not be part of the biometric system
    - Could apply to non-biometric data
    - Moisturizing gel
  - PD: ??

- **Note**
  - If these devices were placed with the intention of impacting data used in a biometric system, they will be considered part of the biometric system.

- **CN: instructions and subject feedback**
  - Instructions and subject feedback to alter presentation
  - Part of the biometric system
  - Examples: take off your glasses

- **CN: Implicit presentation**
  - PD: ???
  - Berlin: NISTIR 7378 considers this term

- **CN: Explicit presentation**
  - PD: ???
  - Berlin: NISTIR 7378 considers this term

- **CN: Cooperative presentation**
  - PD: ???
  - Berlin: NISTIR 7378 considers this term

- **CN: Uncooperative presentation**
  - PD: ???
  - Berlin: NISTIR 7378 considers this term

- **CN: Presentation**
  - Facial expression
  - Rotation of finger
  - Pressure
  - Examples are PE from PIE (pose illumination expression)
  - Subject’s relationship to capture medium

- **CN: frontal presentation**
  - PD: ???

- **CN: right side presentation**
  - PD: ???

- **CN: left side presentation**
  - PD: ???

- **CN: [Physical factors] that impact data capture conditions**
  - Examples:
    - Illuminators and pegs for the hand
    - May or may not be part of the biometric system
    - Could apply to non-biometric data
    - Moisturizing gel
  - PD: ??

- **Note**
  - If these devices were placed with the intention of impacting data used in a biometric system, they will be considered part of the biometric system.

- **CN: instructions and subject feedback**
  - Instructions and subject feedback to alter presentation
  - Part of the biometric system
  - Examples: take off your glasses

- **CN: Subject training**
  - Instructions to subject about usage of device
  - Part of the biometric system
  - Examples: take off your glasses

Problem: at what point does a signal enter the biometric system such that it becomes a biometric signal that can be discussed. We want to give that a name so we can clarify what probe signal and biometric sample are.

Examine all stages of capture sub-system between subject and some stage of processing that we require at this point.
C.7.3.2 Data capture family 2 (may or may not be part of the biometric system)

**CN: biometric capture subsystem**
- Embodies a method for acquiring a signal from a biometric characteristic
- Embodies a process for converting that signal to a biometric sample
- Comprises one or more devices and processes

**PD: biometric capture subsystem**
Proposed defn: biometric capture device(s) and sub-processes required to execute a biometric capture process

**EXAMPLE** In some systems, converting a signal from a biometric characteristic to a biometric sample may include multiple components such as a camera, photographic paper, printer, digital scanner, ink and paper.

Where does this go?
C.7.3.3  Data capture family 3 (may or may not be part of the biometric system)

CN: Biometric capture system
• Input: signal from a biometric characteristic
• Output: biometric sample
C.7.4 Enrolment family

C.7.4.1 Enrolment family 1

**CN: Enrolment**
- a process of creating a record and storing it in a database
- This does not include validation of non-biometric data associated with an individual, a biometric sample, or a biometric reference
- Associate Biometric reference with the data record, which may be empty
  - Associate a biometric reference with a pointer that points to the data record, or
  - Biometric reference becomes an attribute in the data record
- **Input:**
  - Biometric sample(s)
  - Optionally, additional non-biometric data associated with an individual, a biometric sample, or a biometric reference
- **Output:**
  - Biometric Reference and associated enrolment data record / individual’s record
  - no enrolment data record creation
  - data record created

**PD: enrolment**
Proposed defn: registration (deprecated)
the action of enrolling or being enrolled

In Oxford:
- Enrol – officially register
- Enrolment – the action of enrolling or being enrolled

**CN: Re-enrolment**
- Once more to enrol a biometric data subject
- **Reasons:**
  - Changes of biometric characteristics over time
  - Catastrophic change (e.g., lose a finger)
  - Performance degradation (due to major system changes) that cannot be handled by biometric reference adaptation
  - According to system policy
  - Not necessary for the purpose of changing non-biometric data in the data record
  - Procedure may be the same as initial enrolment, but not necessarily (for example, non-biometric data may not need to be re-entered)
- May require linking to the old enrolment data record

**PD: re-enrolment**
Proposed defn: process of establishing a new biometric reference for a biometric data subject already enrolled in the database

**NOTE 1** Re-enrolment requires new captured biometric sample(s).

**NOTE 2** For example, re-enrolment may be required as a result of performance degradation due to major changes in the system or biometric characteristics.

**CN: De-enrolment**
Biometric data record is permanently no longer searchable
- Death /Retirement / Leaving company
- Losing or relinquish privileges implied by authorizations and enrolment
- Expiration of contract or enrolment validity
- Optionally:
  - Removal of the enrolment data record from the database

**PD: de-enrolment**
Proposed defn: permanently exclude biometric data references from biometric processing within the enrolled applications

**Berlin Note:** De-enrolment does not imply that the biometric data records will necessarily be unavailable for all applications

**CN: Enrol**
Create and store, for a biometric capture subject, an enrolment data record associated with that biometric capture subject and including biometric reference and, typically, non-biometric data

**PD: enrol**
Proposed defn: create and store, for a biometric capture subject, an enrolment data record associated with that biometric capture subject and including biometric reference(s) and, typically, non-biometric data

**CN: Re-enrolment**
Create and store, for a biometric capture subject, an enrolment data record associated with that biometric capture subject and including biometric reference and, typically, non-biometric data

**PD: re-enrolment**
Proposed defn: process of establishing a new biometric reference for a biometric data subject already enrolled in the database

**NOTE 1** Re-enrolment requires new captured biometric sample(s).

**NOTE 2** For example, re-enrolment may be required as a result of performance degradation due to major changes in the system or biometric characteristics.
C.7.4.2 Enrolment family 2

CN: biometric reference adaptation
- Incrementally changing or updating the biometric reference through normal usage of the biometric system
- To make better suited for its purpose
- Purpose of biometric reference (used for comparison)
- Template maturity
- To accommodate minor system changes (e.g., may be as a result of changes in the channel, sensor)
- Updating to improve performance to account for changes in biometric characteristics over time
- Possibly automatically
  - Input:
    - biometric reference
    - new biometric sample
  - Output:
    - Better suited biometric reference better suited for comparison

PD: biometric reference adaptation
Proposed defn: automatic/incremental updating of a biometric reference to mitigate performance degradation
NOTE For example, degradation may be from minor changes in the biometric characteristic, channel or sensor.

Does this concept belong here?

CN: biometric reference renewal
- To recover or prevent security problems
- Purpose of biometric reference (used for comparison)
- Updating for security purposes
- Not automatically
- Not done to accommodate changes in the biometric characteristic
- Does not require new biometric sample
- Done when system compromised
  - Input:
    - current biometric reference
    - new secret
  - Output:
    - New biometric reference

PD:
Discussion on renewability – to be inline with "renewing a PIN"

Proposed definition from South Africa. Removed from main body of SD2 after Kyoto as there is still ambiguity that needs to be worked on:
deliberate creation of a transformed biometric reference (3.2.2.9) from an enrolment database to enhance security
NOTE Renewal does not require a new captured biometric sample (3.2.2.2.10.1).

NZ: JP23. It is not necessary to define "Biometric reference Renewal" in SD2, because this term is not related to biometrics itself but security. Delete the concept.

CN: End result of Enrolment
- System message
  - Failure to enrol
  - Enrolment successful
  - Other
- Other data record

PD:
C.7.5 Signal processing family

<table>
<thead>
<tr>
<th>CN: Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Defn:</strong> (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data. [ISO/IEC 18033-1]</td>
</tr>
<tr>
<td>Definition copied from SC27 SD6 (they have more than one definition listed)</td>
</tr>
<tr>
<td>NOTE We do not need to develop this concept, but we need to have the definition so that we understand how it influences the discussion on cancelable biometrics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Defn:</strong> Reversal of a corresponding encryption [ISO 18033-1]</td>
</tr>
<tr>
<td>Definition copied from SC27 SD6 (they have more than one definition listed)</td>
</tr>
<tr>
<td>NOTE We do not need to develop this concept, but we need to have the definition so that we understand how it influences the discussion on cancelable biometrics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: intermediate biometric sample processing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PD:</strong> intermediate biometric sample processing</td>
</tr>
<tr>
<td>Proposed defn: any manipulation of a biometric sample that does not produce biometric features</td>
</tr>
<tr>
<td>EXAMPLE Examples of intermediate processing include cropping, down-sampling, compression, conversion to data interchange formats standard and image enhancement</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: feature extraction process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proposed defn:</strong> process applied to a biometric sample with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other biometric samples</td>
</tr>
<tr>
<td>NOTE 1 Filters applied to biometric samples are not themselves biometric features, however the output of the filter applied to these samples may be. Therefore, for example, eigenfaces are not biometric features.</td>
</tr>
<tr>
<td>NOTE 2 Repeatable implies low variation between outputs generated from biometric samples of the same biometric data subject.</td>
</tr>
<tr>
<td>NOTE 3 Distinctive implies high variation between outputs generated from biometric samples of different biometric data subjects.</td>
</tr>
<tr>
<td>NOTE 4 An uncompleted biometric feature extraction process might be an error message or a NULL vector.</td>
</tr>
<tr>
<td><strong>NOTES</strong></td>
</tr>
<tr>
<td>• Eigenfaces are not features – they are the extraction process and not the outcome</td>
</tr>
<tr>
<td>• Features are to templates as XXX is to models as YYY is to &lt;images/signals&gt;</td>
</tr>
<tr>
<td>• Identity transform can be applied to a signal to produce features</td>
</tr>
<tr>
<td>• Acknowledge the issue where a system transforms the sample to a number at enrolment. At verification the transform is applied to the probe sample to generate a number again. That number is output from the system with no comparison occurring.</td>
</tr>
</tbody>
</table>
C.8 Interacting

C.8.1 Interacting 1

**CN:** biometric claim
- Can be specific or unspecific
- Can be 1st, 2nd or 3rd person
- Has to do with who was the source or not the source of unspecific or specific biometric references in a database
- Source = same biometric data subject and of the same biometric characteristic

**PD:** biometric claim
Proposed defn: claim that a biometric capture subject is or is not the source of a specified or unspecified biometric reference in a biometric enrolment database

**NOTE 1**
A biometric claim can be made by any user of the biometric system.

**NOTE 2**
The phrase "claim of identity" is often used to label this concept.

**NOTE 3**
Claims may be positive – i.e. that the biometric capture subject is enrolled; negative – i.e. that the biometric capture subject is not enrolled, specific – i.e. that the biometric capture subject is or is not enrolled as a specified enrollee; or non-specific – i.e. that the biometric capture subject is or is not among the set or subset of enrollees.

**NOTE 4**
Biometric claims are not necessarily made by the subject.

**NOTE 5**
The biometric reference could be on a database, card or distributed throughout a network.

**History:**
Note 5 added and Note 4 changed from: "Biometric claims can be made in the 1st, 2nd or 3rd person" in Berlin.

**Claim:** Oxford: assert that something is the case; an assertion of the truth of something

---

**CN:** Positive claim
- Examples: I am in the database; I am Jane Smith
- [Truth of claim is not a characteristic of positive claim]
- Assertion that a biometric capture subject () is the source of a specified or unspecified biometric reference in a biometric enrolment database

**PD:** positive biometric claim
Defn: assertion that a biometric capture subject () is the source of a specified or unspecified biometric reference in a biometric enrolment database

---

**CN:** Negative claim
- Examples: I am not in the database; I am not Jane Smith
- [Truth of claim is not a characteristic of negative claim]
- Assertion that a biometric capture subject () is not the source of a specified or unspecified biometric reference in a biometric enrolment database

**PD:** negative biometric claim
Defn: assertion that a biometric capture subject () is not the source of a specified or unspecified biometric reference in a biometric enrolment database

---

**NZ:** Keep for history: removed genuine claim, true biometric claim, false biometric claim, impostor claim, defrauder claim – deciding instead to concentrate on definitions of roles.

**NZ:** Not really happy with terms: positive claim and negative claims (is this a correct statement?)
C.8.2 Interacting 2

<table>
<thead>
<tr>
<th>CN</th>
<th>Concept name</th>
</tr>
</thead>
<tbody>
<tr>
<td>PD</td>
<td>Preliminary designation</td>
</tr>
<tr>
<td>CN: Correctly affirm unspecified positive biometric claim and returning true identifier</td>
<td></td>
</tr>
<tr>
<td>PD: Identification</td>
<td></td>
</tr>
<tr>
<td>CN: Correctly affirm positive biometric claim</td>
<td></td>
</tr>
<tr>
<td>PD: True Verification</td>
<td></td>
</tr>
<tr>
<td>CN: Correctly affirm negative biometric claim</td>
<td></td>
</tr>
<tr>
<td>PD: True Confirmation of Negative Claim</td>
<td></td>
</tr>
<tr>
<td>CN: Correctly deny positive biometric claim</td>
<td></td>
</tr>
<tr>
<td>PD: True Rejection</td>
<td></td>
</tr>
<tr>
<td>CN: Correctly deny negative biometric claim</td>
<td></td>
</tr>
<tr>
<td>PD: True Contradiction of Negative Claim</td>
<td></td>
</tr>
<tr>
<td>CN: Correctly deny unspecified negative biometric claim and returning true identifier</td>
<td></td>
</tr>
<tr>
<td>PD: Identification</td>
<td></td>
</tr>
</tbody>
</table>

Associative relation:
- Characteristics developed by WG1
- Characteristics need further development by WG1

- Essential characteristic
### C.8.3 Interacting 3

<table>
<thead>
<tr>
<th>CN: Incorrectly affirm unspecific positive biometric claim and returning wrong identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A positive biometric claim that has been wrongly shown to be true using biometric means (Type II error – Neyman and Pearson)</td>
</tr>
<tr>
<td>• Returning wrong identifier</td>
</tr>
<tr>
<td>PD: False Identification</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: Incorrectly affirm positive biometric claim</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A positive biometric claim that has been wrongly shown to be true using biometric means</td>
</tr>
<tr>
<td>PD: False acceptance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: Incorrectly affirm negative biometric claim</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A negative biometric claim that has been wrongly shown to be true using biometric means</td>
</tr>
<tr>
<td>• Type II error – Neyman and Pearson ?</td>
</tr>
<tr>
<td>• PD: False positive identification error – ISO 19795 Part 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: Incorrectly deny positive biometric claim</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A positive biometric claim that has been incorrectly shown to be false using biometric means</td>
</tr>
<tr>
<td>• Type I error – Neyman and Pearson ?</td>
</tr>
<tr>
<td>PD: False rejection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: Incorrectly deny negative biometric claim</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A negative biometric claim that has incorrectly been shown to be false using biometric means</td>
</tr>
<tr>
<td>PD: False negative identification error – ISO 19795 Part 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CN: Incorrectly deny unspecific negative biometric claim and returning wrong identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A negative biometric claim that has incorrectly been shown to be false using biometric means</td>
</tr>
<tr>
<td>• Returning a false identifier</td>
</tr>
<tr>
<td>PD:</td>
</tr>
</tbody>
</table>

NZ: We may be able to massage the words so that claim does not appear in the performance definitions (except for False Accept and False Reject) - in the same way we have avoided using impostor in the match and non-match error terms.
C.8.4 Interacting 4

CN: Impostor verification attempt
• a verification attempt in which the identity of a non-self enrollee is claimed.
• Can be zero-effort, or motivated impostor attempts
PD:
Defn: a verification attempt in which the identity of a non-self enrollee is claimed
NOTE There are zero-effort and motivated impostor transactions.

CN: Genuine verification attempt
• an attempt to verify a genuine claim, making best efforts to match the corresponding biometric reference
PD:
Defn: a transaction carried out in order to verify a genuine claim, making best efforts to match the corresponding biometric reference

CN: Live capture
• <to be developed, moved or removed>
PD:
Defn: capture
Oxford defn: record or express accurately in words or pictures; cause data to be stored in a computer
This concept also appears in “data capture family” sub-field of “functioning”
C.8.5 Concept map from previous version of SD2 – use when developing "Interacting" concept map

Concept: management of identity with biometric system
Term: Class of Identity <Identity & ID>

Nature of the Claim

Truth of the Claim

Concept: a genuine person
Term: A genuine claim

Concept: a non-genuine person
Term: ???

Concept: claim to be in the database
Term: a positive claim

Concept: claim not to be in the database
Term: a negative claim

Concept: not making an overt claim
Term: an implicit claim

Concept: claiming an identity
Term: an explicit claim

Criteria

Truth of the Claim

Nature of the Claim

23 – genuine claim
**Claim does not always have to be made by the claimant, it could be made about the subject.

22 - Negative explicit claim

21 - Positive explicit claim

25 – defrauder claim
Recommendation: replace defrauder w/ fraudulent claim

24 – impostor claim
Where does this belong?
For comment: Is this framework correct?
Intentional > false > positive > explicit

2 - passive attack
Recommendation: **defined to be 2 different things??

Non-Zero Effort

Zero Effort

Concept: an inadvertent claim including a mistake
Term: ???

Concept: Intentional non-genuine claim
Term: A fraudulent claim

Concept: positive claim to an existing identity
Term: ???

Concept: negative claim to an existing identity
Term: a disruptor claim

Concept: the identity is unknown
Term: an imposter claim

Concept: the identity is known
Term: an usurper claim

© ISO/IEC 2006 – All rights reserved 61
C.8.6 Concept map from previous version of SD2 – use when developing "Interacting" concept map
C.9 Personnel

Sub-sub-field: General

Sub-sub-field: Subjects
C.9.1 Subjects

C.9.1.1 Subjects 1

CN: Subject
- Any individual whose biometric characteristics have been captured for the use of biometric recognition by a system
  - Subject of the query as opposed to the operator
  - People who have enrolled
  - Deliberate impostors
  - Passers by who don’t know their biometric characteristics have been captured
  - Individuals who have their biometric characteristics captured without their knowledge
  - Any individual where involved in an attempt

PD: subject
Proposed defn:
NOTE 1 Use in the natural language sense.
NOTE 2 An individual undergoing a biometric process is typically referred to as a biometric subject, further qualified by the type of process. For example, biometric capture subject and biometric data subject. This helps clarify the different roles of individuals, such as attendants and biometric capture subjects.

History:
Subject: May have privacy problems in some instances – when used similar to “objects”, connotation of subservient

Oxford: subject – a person or thing that is being discussed or dealt with or give rise to something; a person who is the focus of scientific or medical attention or experiment
A distinctive or original person

London: DE.3: Decide on definition to include in main body

CN: Biometric data subject
- Subject’s data is within the biometric system
- Individual with any form of individualized biometric data in the system (does not include those people who supplied data to be incorporated in models) (i.e., aggregated data from many individuals for use in Universal Background Model – may need another term for these subjects)
- No longer a subject once biometric data is removed from the system
- Regardless of level of participation by the individual
  - The biometric data capture subject’s sample is compared with the biometric data subject’s reference

PD: biometric data subject
Proposed defn: individual whose individualized biometric data is within the biometric system
NOTE The intent of the word “individualized” is to distinguish biometric data subjects from those whose aggregated data was used in the creation of the biometric recognition algorithm. Examples of individuals contributing biometric data who are not biometric data subjects include those who contributed to a Universal Background Model in speaker recognition systems, or who contributed to the creation of an eigenface basis set in a facial recognition system.

CN: subject of an interaction (biometric capture subject)
- Individuals where the system is trying to capture their biometric characteristics
- Subject of the biometric capture process
- Capture process need not be successful
- Can be a data capture subject regardless of intent
- Does not matter if they are genuine or impostor; subject regardless of ground truth
- When the capture process is finished, the individual is no longer a biometric data capture subject

PD: biometric capture subject
Proposed defn: individual who is the subject of a biometric capture process
NOTE The subject remains a biometric capture subject only during the biometric capture process.

History:
Proposed defns:
- Individual of whom the biometric capture subsystem is collecting or attempting to collect a signal from their biometric characteristic
- Individual interacting with a biometric capture subsystem for the purpose of collecting (generating?) their biometric sample
- When a biometric capture subsystem attempts to collect a biometric signal form an individual, that person is a subject
- Individual whose biometric characteristic is interacting …
- Individual of whom the biometric capture subsystem is collecting or attempting to collect a signal for the purpose of generating a biometric sample

Oxford: interaction – 2 entities mind and body each affecting each other; allowing a 2 way flow; reciprocal

Berlin Note: These Definitions are Appropriate for Subjects of Operational Systems.

Test Subjects Currently Treated in WG5
C.9.1.2 Subjects 2

**CN: Subversive users**  Berlin Note we do mean subjects, users, operators, legal persons etc
- Intent to subvert system policy
- Act may not be illegal or immoral
- Actively seeking to use some aspects of the system improperly or to exploit system errors
- May attack the system at any level

**PD: Subversive user**
Proposed defn: user of a biometric system who attempts to subvert the correct and intended system policy

**EXAMPLE** Operator letting unsanctioned subject through, administrators allowing unsanctioned function creep, subjects impersonating enrolled users.

Oxford defn: Subversive: Seeking or intending to subvert an established system or institution

**CN: Someone in Disguise**
- Capture Subject trying not to be matched to someone else’s record

**PD: Impostor**
Oxford defn: person who assumes a false identity in order to deceive or defraud

**CN: Impostor**
- The impostor can be further qualified according to the level of skill, resources, time deployed this includes zero effort, active impostor. The definition of level of skill etc are outside the scope of WG1

**CN: Avoider**
- Non-cooperative intent
- Doesn’t interact with biometric system – therefore not a biometric capture subject
- Negative and positive systems
- Circumvention
- May or may not be fraudulent

NOTE A avoider can bypass a biometric system (3.2.1.2) through any form of social engineering (bribery, for example).

Berlin Note: this concept is left in the concept map to illustrate that there are subversive subjects who are not data capture subjects.

**History:** Following concepts removed at Berlin meeting:
- casual impostor (zero-effort impostor)
- motivated impostor
- deceiver / impostor (negative claim system)
- impersonator / impostor (positive claim system)
- unintentional impostor (with note: imposters cannot be unintentional therefore we don’t need this term)
- subversive <people other than subjects>
- Good subjects (and all concepts that were below good subjects)
C.9.2  General

C.9.2.1  General 1

**CN: User**
- Any Person involved with the operation, collection, administration, ownership, use of results.
- Person that interacts in some way with the biometric system.

**PD: user (of a biometric system)**
Proposed defn: any person or organization interacting in any way with a biometric system.

**NOTE** When discussing a particular class of users involved with biometric systems, the specific term for that class should be used. For example, those users whose biometric data is being collected should be referred to as biometric capture subjects.

**History**
- suggests active involvement
- could be confused with system owner / operator / administrator

**Oxford defn:** a person who uses or operates something.

**CN: End user**

**PD:**
Proposed defn: Deprecated
Note: "End user" suggests active involvement and could be confused with system owner, operator, administrator, biometric subject.

**CN: biometric system operator**

**PD: biometric system**
Proposed defn: Person(s) who executes policies and procedures in the administration of a biometric system.

**CN: biometric system owner**
- Holds overall responsibility to acquire, implement and operate biometric system.
- Accountability for biometric system.

**PD: biometric system owner**
Proposed defn: Person(s) with overall accountability for the acquisition, implementation and operation of the biometric system.

(i.e., Immigration and Nationalities Directorate)

**CN: Attendant / Supervisor**
- Individual controlling the biometric system.
- Biometric capture subject is present.

**PD: Attendant**
Proposed defn: agent of the system operator who directly interacts with the biometric capture subject.

Example: immigration officer supervising biometric capture process and taking action on the comparison decision.
C.9.2.2 General 2

**CN: Applicant**
- Someone seeking to be an enrollee
- Used in natural language sense

**PD: Applicant**
Proposed defn: an individual (A.11.4) who applies for something

**NOTE 1** Definition source: Oxford dictionary
**NOTE 2** The dictionary definition has been modified from “person” to “individual” for consistency with ([ISO/IEC 15944-1:2002 (3.47)])

[NZ: Editor’s note: Suggest adding the following clarification sentence to this note: “For biometrics purposes, applicants are “natural persons” not “legal persons”, see Person (A.11.x).”]

**CN: biometric enrollee**
- Biometric data subject whose biometric data is held into a biometric enrolment database
- Consent / knowledge not necessary
- Once the biometric data is removed from the biometric enrolment database, the individual is no longer an enrollee

**PD: biometric enrollee**
Proposed defn: biometric data subject whose biometric data is held in a biometric enrolment database

[NZ: Change enrollee to biometric enrollee]

**CN: Unknown Person**
- A specific biometric identity
- Not enrollee

**PD: (not enrollee) <Identity>**

**CN: Claimant**
- A person making a claim
- Claim can be positive or negative
- Can make a claim on someone’s behalf

**PD: Claimant**
Oxford: <word is there, but no definition>

**History:**
- 2 possibilities:
  - The claimant need not be the subject of the claim (i.e. A police officer making comparisons between a latent print and references in the database – police officer is the claimant)
  - Subject about who the claim is made (more consistent with current usage) (i.e. A police officer making comparisons between a latent print and references in the database – source of the latent is the claimant)

WG1 will try and seek opinions from others in the industry on what is generally used/accepted.

**Notes from previous A.4.1.2:**
- Applicant and Claimant seem to be homonym
- An ambiguity is pointed on claimant: to be solved
- Goat / goats seems to be non-essential characteristic of applicant
C.10 Application

C.10.1 Application 1

ISO/IEC WD 2.8

© ISO/IEC 2006 – All rights reserved
C.10.2 Application 2

**CN: biometric recognition**
- «to be developed, moved or removed»

**PD: biometric recognition**

Editor’s note: added in response to JP14 comment to NZ meeting that “biometric recognition” is a preferred term over authentication. Do we need the concept of biometric recognition then? If so it needs to be added to main body of SD2. Also, does it belong here.

Berlin Note: the definition of biometrics includes the term and word recognition.

**CN: Special Treatment**
- Occurs with a false rejection
- “Plan B”, fallback (deprecated)
- Exception handling
- «to be developed, moved or removed»

**PD: special treatment**

---

**Associative relation**

- Characteristics developed by WG1
- Characteristics need further development by WG1

**CN** Concept name

**PD** Preliminary designation

- Essential characteristic

History: following concepts have been deprecated (see main body notes):
- authentication (as a synonym for biometric verification or biometric identification)
- negative identification
- positive identification
C.11 Performance

C.11.1 Performance 1 (working slide)

Processes that may fail:
- Capture process
- Enrollment process
- Comparison process
- Transmission process
- Decision process
- Storage process

Types of performance:
- Where we have defined a process
- Must be measurable

2 types of failure
- Gets to end of program or
- Doesn’t

Performance
- Needs a unit of measure
- What is the denominator
- Failure to process = failure to complete

Capture
Enrollment
Feature Extraction

Correct result
Incorrect result
No result: Abortive attempt: Failure to complete the process

False positive
False negative

False match
False non-match

False verified
False not verified
No result

Generalized False acceptance
Generalized False rejection
### C.11.2 Performance 2 (working slide)

**System Response**

<table>
<thead>
<tr>
<th>Process</th>
<th>False positive</th>
<th>False negative</th>
<th>No result: Abortive attempt: Failure to complete the process</th>
</tr>
</thead>
</table>

**Verification**

- False Accept
- False Reject

**Identification**

- False Positive
- Identification Error
- False Negative
- Identification Error

**Notes:**
- We want a population average

---

**Notes:**

- Biometric capture subject – the individual in front of the capture device
- Biometric data subject – individual from which successfully a biometric sample was generated
- Enrollee – individual from whose biometric sample, biometric features were successfully extracted and a reference created and stored. Only an enrollee while that reference is stored and active

**Biometric capture subject**

individual who is the subject of a biometric capture process (3.2.4.3.1)

Note: The subject remains a biometric capture subject only during the biometric capture process.

**Biometric data subject**

individual whose individualized biometric data (3.2.2.2.2) is within the biometric system (3.2.1.2)

**NOTE**

The intent of the word “individualized” is to distinguish biometric data subjects from those whose aggregated data was used in the creation of the biometric recognition algorithm. Examples of individuals contributing biometric data (3.2.2.2.2) who are not biometric data subjects include those who contributed to a Universal Background Model in speaker recognition systems, or who contributed to the creation of an eigenface basis set in a facial recognition system.

**Enrollee**

biometric data subject (3.4.3) whose biometric data (3.2.2.2.2) is held in a biometric enrolment database (3.2.2.1.1)
C.11.3 Performance 3

4 possible cases, compare:
• Same individual/Same characteristic – can have false non-match or abortion
• Same individual/Different characteristics – false match + potential for ambiguity depending on how characteristic is defined
• Different individuals / same characteristics – false match
• Different individuals / different characteristics – false match

CN: biometric non-match trials (impostor trials)
• a set of comparisons of biometric samples and biometric references from:
  - Same biometric data subject / different biometric characteristics; and/or
  - Different biometric data subjects/ same biometric characteristics; and/or
  - Different biometric data subjects / different biometric characteristics.
• The possible results of a biometric non-match trial can be non-match (true), match (false), or failure to process.

PD: biometric non-match trials (previously referred to as “impostor trials”)
Proposed defn: set of comparisons of biometric samples and biometric references from different biometric data subjects

Note 1: If a decision of “match” for a recognition biometric sample and a biometric reference from different biometric data subject is considered to be a false match then the non-match trials would also include such comparisons.
Note 2: Non-match trials do not fully model the case where a biometric capture subject is trying not to be recognized.
Note 3: A non-match trial need not contain all possible comparisons of biometric samples and biometric references from different biometric capture subject characteristics.

CN: biometric match trials (genuine trials)
• a set of comparisons of biometric samples and biometric references from:
  - Same biometric data subject / same biometric characteristics
• The possible results of a biometric match trial can be match (true), non-match (false), or failure to process.

PD: biometric match trials (previously referred to as “genuine trials”)
Proposed defn: set of comparisons of biometric samples and biometric references from the same biometric data subjects and the same biometric characteristics.

Note 1: Biometric match trials do not fully model the case where a biometric capture subject is trying not to be recognized.
### C.11.4 Performance 4

#### CN: False match
- No claim at this level
- The system falsely matches the recognition biometric sample to the biometric reference.
- Cases where a match is found for:
  - Different biometric capture subjects
  - And, possibly, different characteristics of the same biometric capture subject (e.g., matching different fingers of the same person may be considered a false match, while matching a mispronounced pass-phrase in text-dependent speaker recognition might be considered a correct match)
- Excludes failure to acquire

#### PD: False match
Proposed defn: comparison decision of “match” for a recognition biometric sample and a biometric reference that are from different biometric data subjects

Note 1: It is recognized that this definition considers only the false match at the subject level and not at the characteristic level. Sometimes a comparison decision of “match” for a recognition biometric sample and a biometric reference from different biometric characteristics of the same biometric data subject is also considered to be a false match. For example, a match decision when comparing Galton ridges of different fingers of the same biometric data subject might be considered a false match, while a match decision for a mispronounced pass-phrase in text-dependent speaker recognition might be considered a correct match.

#### CN: False non-match
- No claim at this level
- The system fails to match the recognition biometric sample to the biometric reference
- Case where a fail to match is found for:
  - Same biometric capture subject and same biometric characteristic.
- NOTE Excludes Failure to acquire
- May be ambiguity in how much mis-action on the part of the biometric capture subject is tolerated before it is considered to be the presentation of a different biometric characteristic

#### PD: False non-match
Proposed defn: comparison decision of “non-match” for a recognition biometric sample and a biometric reference that are from the same biometric data subject and of the same biometric characteristic.

Note 1: There may need to be consideration on how much mis-action on the part of the biometric capture subject is tolerated before the recognition biometric sample and the biometric reference are deemed to be of different biometric characteristics.
C.11.5 Performance 5

**CN: biometric failure to enrol**
- Enrolment transaction failure
- Failure to capture biometric features usable for biometric comparison
- Failure to generate a usable biometric reference
- Can be due to:
  - Failure to capture
  - Failure to extract usable biometric features
  - Failure to generate a usable biometric reference
- Exclude: procedural failures, policy decision, any determination based on non-biometric data
- Exclude abortions due to false matches
- Measure of what percentage of population is eligible to enrol but cannot enrol
- No enrolment data record created or stored
- Note: this failure could be an automatic or manual decision
- Include failures due to lack of required biometric characteristic

**PD: biometric failure to enrol**
- Proposed defn: Failure of the biometric system to store a usable biometric reference due to deficiencies in the biometric data during enrolment
- Note: Deficiencies in the biometric data manifested as failure to capture, failure to extract features usable for biometric reference generation, or failure to generate a usable biometric reference.

**CN: biometric failure to enrol rate**
- Proportion of biometric enrolment sessions (sessions = one or more attempts)
- In accordance with policy governing quality, number of enrolment attempts etc.
- Denominator: number of biometric enrolment sessions; excluding those sessions that failed to complete for non-biometric reasons
- Numerator: number of biometric failures to enrol

**PD: biometric failure to enrol rate**
- Proposed defn: Proportion of biometric enrolment sessions (that did not fail for non-biometric reasons), that resulted in a biometric failure to enrol
- Note 1: Basing the denominator on the number of biometric enrolment sessions may result in a higher value than basing it on the number of biometric capture subjects.
- Note 2: The proportion denominator is the number of biometric enrolment sessions, excluding those sessions that failed to complete for non-biometric reasons.

---

**biometric enrollee**
biometric data subject whose biometric data is held in a biometric enrolment database

**enrolment data record**
record created upon enrolment, associated with the biometric data subject and including biometric reference(s) and typically non-biometric data

**enrolment**
registration (deprecated)
the action of enrolling or being enrolled

**enrol**
create and store, for a biometric capture subject, an enrolment data record associated with that biometric capture subject and including biometric reference(s) and, typically, non-biometric data

---

**Manifest**
(adj) clear and obvious
(v) show, demonstrate, become apparent

---

NZ: FYI. Note on denominator has been added for clarity.
### C.11.6 Performance 6

<table>
<thead>
<tr>
<th>CN: Failure to acquire rate for enrolment</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Biometric application = enrolment</td>
</tr>
<tr>
<td>• Proportion of enrolment attempts for which there is a failure to acquire</td>
</tr>
<tr>
<td>• EXAMPLE – If everyone enrols on 2nd attempt, FTE = 0 but FTA(enrol) = 50%.</td>
</tr>
</tbody>
</table>

**PD:**
Proposed defn: failure to acquire rate where the [biometric application] is enrolment

<table>
<thead>
<tr>
<th>CN: Failure to acquire</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Either a failure to capture, or</td>
</tr>
<tr>
<td>• a failure to extract biometric features usable for biometric comparison or biometric reference generation as a result of deficiencies in the biometric data</td>
</tr>
<tr>
<td>• [useful = (Oxford) able to be used for practical purpose; (Japan) convenient; (RF) helpful/good]</td>
</tr>
<tr>
<td>• [usable = (Oxford) able to be used (RF, JP prefer this)] – WG1 accepts</td>
</tr>
</tbody>
</table>

**PD:**
Proposed defn: either a failure to capture () or a failure to extract biometric features usable for biometric comparison or biometric reference generation due to deficiencies in the biometric data

<table>
<thead>
<tr>
<th>CN: Failure to capture</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Can occur during any biometric application (possibly many times per person)</td>
</tr>
<tr>
<td>• When the system fails to capture a biometric sample usable for biometric comparison or biometric feature generation</td>
</tr>
<tr>
<td>• usable (e.g. meeting ISO standards, …)</td>
</tr>
<tr>
<td>• [OK with the ambiguity that this concept does not distinguish between system failures and failures due to biometric data deficiencies]</td>
</tr>
<tr>
<td>• Failures as a result of deficiencies in the biometric data</td>
</tr>
</tbody>
</table>

**PD:**
Proposed defn: biometric capture process that does not result in the creation of a usable biometric sample due to deficiencies in the biometric data

<table>
<thead>
<tr>
<th>CN: Failure to acquire rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Can be attributed to any biometric application</td>
</tr>
<tr>
<td>• Proportion</td>
</tr>
<tr>
<td>• Numerator: total attempts resulting in a failure to acquire</td>
</tr>
<tr>
<td>• Denominator: total number of attempts; excluding those attempts that failed to complete for non-biometric reasons</td>
</tr>
</tbody>
</table>

| **PD:**
Proposed defn: proportion of the [biometric application] attempts (that did not fail for non-biometric reasons), that result in a failure to acquire |

| Note: The proportion denominator is the number of biometric enrolment attempts, excluding those attempts that failed to complete for non-biometric reasons. |

| NZ: FYI, the Note has been added for clarity |
C.11.7 Performance 7

CN: open set identification system
- Returns a candidate list
- Pointers returned
- Not everyone enrolled
- False negatives exist

PD:

CN: open zero identification system
- Candidate list can be empty
- In the event that only a binary indicator is returned based on the existence of a non-null candidate list then the system is a verification system
- In the event that a binary indicator and the pointers are returned
- These systems can have false positive errors

PD:

CN: open non-zero identification system
- Candidate list cannot be empty
- These systems cannot have false positives

PD:

Editor's question: out of Berlin, were these meant to be included in the “Performance” concept map – or here for information only? I have not added them to the SD2 main body yet. <Delete note following Tel Aviv meeting>
C.11.8 Performance 8

**CN: open set identification error**
- An incorrect result
- Nature of result is a candidate list (i.e., subset of all enrolled references)
- Length of candidate list is determined by system policy
- Likelihood of identification errors depends on parameters such as thresholds and length of candidate list
- When executing biometric identification function
  - Any size candidate list, as determined by the identification function

**PD:**

**CN: combination identification error**
- The biometric capture subject has a reference in the system
- Person who should be identified is not (i.e., their reference identifier is not returned in the candidate list produced by the identification function)
- Non-empty list returned
- Can only occur in open zero identification systems
- <Common use: mis-identification>

**PD:**

**Defn:** identification function output of a candidate list that does not contain the biometric reference identifier of the biometric capture subject when the biometric capture subject is enrolled

**Note (for WG1): this concept might be generalized to talk about CMC curves.**

**CN: false-negative open set identification error**
- This can only occur if the biometric capture subject has a reference in the system
- The error occurs when the a pointer to the biometric capture subject is not in the candidate list
- Person who should be identified is not (i.e., their reference identifier is not returned in the candidate list produced by the identification function)
- Empty list may be returned

**PD:**

**Defn:** proportion of the completed biometric mated identification trials that results in a false-negative identification error

**CN: open set identification error trials (mated)**
- [Mate] in the database
- Expect people to be identified
- Set of trials
- Selected to compute false-negative identification errors (reference 19795-1)
- Recognition sample, apply identification function, check to see if candidate list returned contains reference identifier of biometric capture subject, if not, count this as a false-negative identification error
- Each trial returns either 1 error or no errors

**PD:**

**Berlin Note:** consider CM Sub field performance 3 boxes concepts: biometric non-match trials (impostor trials) and biometric match trials (genuine trials)

**CN: false-negative open set identification error trials (no mate)**
- [Mate] not in database
- Expect people not to be identified
- Set of trials
- Selected to compute false-positive identification errors (reference 19795-1)
- Recognition sample, apply identification function, check to see if candidate list returned is empty, if not, count this as a false-positive identification error
- Each trial returns either 1 error or no errors
- May not have value in open non-zero identification systems

**PD:**

**Berlin Note:** consider CM Sub field performance 3 boxes concepts: biometric non-match trials (impostor trials) and biometric match trials (genuine trials)

**CN: open set false-negative identification error rate**
- [Mate] not in database
- Expect people not to be identified
- Set of trials
- Numerator: number of false-negative identification errors within the trials
- Denominator: number of identification trials

**PD:**

**Defn:** proportion of completed biometric non-mated identification trials that result in a false-negative identification error

**CN: false-positive open set identification error**
- Will only be defined by WG1 for open zero identification system
- Users of open non-zero systems may wish to come up with their own definitions of false-positive identification errors
- Occurs when candidate list is not empty and
  - Subject is not in database
  - And possibly occurs when candidate list is not empty and
    - Subject is in the database but not in candidate list
      - Combination of false positive and negative
      - This is a special type of case that will require special treatment.
      - Subject is in the candidate list and other candidates are too. Whether this would be regarded as a false positive may depend on details of the application.

**PD:**

**CN: false-positive open set identification error trials (no mate)**
- [Mate] not in database
- Expect people not to be identified
- Set of trials
- Selected to compute false-positive identification errors (reference 19795-1)
- Recognition sample, apply identification function, check to see if candidate list returned is empty, if not, count this as a false-positive identification error
- Each trial returns either 1 error or no errors

**PD:**

**Berlin Note:** consider CM Sub field performance 3 boxes concepts: biometric non-match trials (impostor trials) and biometric match trials (genuine trials)

**CN: open set false-positive identification error rate**
- [Mate] not in database
- Expect people not to be identified
- Set of trials
- Numerator: number of false-positive identification errors within the trials
- Denominator: number of identification trials

**PD:**

**Defn:** proportion of completed biometric non-mated identification trials that result in a false-positive identification error
C.11.9 Performance 9

CN: closed set identification error
• An incorrect result
• When executing biometric identification function
• Any size candidate list, as determined by the identification function

CN: closed set combination identification error
• The biometric capture subject has a reference in the system
• Person who should be identified is not (i.e., their reference identifier is not returned in the candidate list produced by the identification function)
• Non-empty list returned
  • <Sometimes gets included as a false-hit>
  • <Common use: mis-identification>

PD:

Defn: identification function output of a candidate list that contains at least one biometric reference identifier when the biometric capture subject is not enrolled

Note (for WG1): this concept might be generalized to talk about CMC curves.

CN: false-positive identification error
• The biometric capture subject does not have a reference in the system
• Person who should not be identified (i.e., a reference identifier is returned in the candidate list produced by the identification function)
• Open-set identification system
• <Common use terms: false-hit; false accept>

PD:

Defn: identification function output of a candidate list that does not contain the biometric reference identifier of the biometric capture subject when the biometric capture subject is enrolled

Note: When a biometric capture subject is not enrolled, the only non-error condition is to return an empty candidate list.

CN: false-negative identification error
• The biometric capture subject has a reference in the system
• Person who should be identified is not (i.e., their reference identifier is not returned in the candidate list produced by the identification function)
• Open-set identification system
• Empty list may be returned
  • <Common use: false-miss; false reject>

PD:

Defn: identification function output of a candidate list that does not contain the biometric reference identifier of the biometric capture subject when the biometric capture subject is enrolled

Note (for WG1): this concept might be generalized to talk about CMC curves.

CN: closed set combination false-negative identification error
• The biometric capture subject has a reference in the system
• Person who should be identified is not (i.e., their reference identifier is not returned in the candidate list produced by the identification function)
• Non-empty list returned
  • <Sometimes gets included as a false-hit>
  • <Common use: mis-identification>

PD:

Defn: identification function output of a candidate list that does not contain the biometric reference identifier of the biometric capture subject when the biometric capture subject is enrolled

Note (for WG1): this concept might be generalized to talk about CMC curves.

CN: closed set false-negative identification error trials
• [Mate] in the database
• Expect people to be identified
• Set of trials
• Selected to compute false-negative identification errors (reference 19765-1)
• Recognition sample, apply identification function, check to see if candidate list returned contains reference identifier of biometric capture subject, if not, count this as a false-negative identification error
• Each trial returns either 1 error or no errors

PD:

Defn:

CN: closed set false-negative identification error rate
• [Mate] in the database
• Expect people to be identified
• Set of trials
• Numerator: number of false-negative identification errors within the trials
• Denominator: number of identification trials

PD:

Defn: proportion of the completed biometric mated identification trials that results in a false-negative identification error

CN: False match
• No claims at this level
• the system falsely matches the recognition biometric sample to the biometric reference.
• Cases where a match is found for:
  - Different biometric capture subjects
  - And, possibly, different characteristics of the same biometric capture subject (eg. Matching different fingers of the same person may be considered a false match, while matching a mispronounced pass-phrase in text-dependent speaker recognition might be considered a correct match)
  - Excludes Failure to acquire

PD: false match

Proposed defn: comparison decision of "match" for a recognition biometric sample and a biometric reference that are from different biometric data subjects

Note 1: Sometimes a decision of "match" for a recognition biometric sample and a biometric reference from different biometric characteristics of the same biometric data subject is also considered to be a false match. For example, a match decision when comparing Galton ridges of different fingers of the same biometric data subject might be considered a false match, while a match decision for a mispronounced pass-phrase in text-dependent speaker recognition might be considered a correct match.
C.11.10 Performance 10

**Editor's note:** concepts in this concept map to be added to SD2 main body following further development in Tel Aviv. Note to be deleted following Tel Aviv meeting.

**biometric claim**
assertion that a biometric capture subject () is or is not the source of a specified or unspecified biometric reference (3.2.2.8) in a biometric enrolment database

**CN: Type I error about a biometric claim**
false negative
• Fail to accept as true (reject) a biometric claim that is true
• True biometric claim
• No decision, no error
• PD: Type I error

**CN: Type II error about a biometric claim**
false positive
• Accept a claim that is false
• False biometric claim
• No decision, no error
• PD: Type II error

**CN: errors from an open-set identifications system where no claim is made**
• Identification system
• No claim is made
• Cases (ground truth):
  • [1] database has a biometric reference for the subject
  • [2] database does not have a biometric reference for the subject
• Case 1: there is an error if the candidate list does not contain the reference (candidate list has an implicit assumption of thresholding)
• Case 2: there is an error if the candidate list is not empty
• PD:
  open-set identification (biometric application)
application that determines a possibly empty candidate list by collecting one or more biometric samples from a biometric capture subject and searching the enrolment database for similar biometric references

Argument: the "thresholding" note in case [1] implies a claim is in fact being made and thus this concept is inconsistent.

**CN: errors from a closed-set identifications system where no claim is made**
• No claim is made
• Cases (ground truth):
  • [1] database has a biometric reference for the subject
  • [2] database does not have a biometric reference for the subject
• Case 1: there is an error if the candidate list does not contain the reference (candidate list has an implicit assumption of thresholding)
• Case 2: there is an error if the candidate list is not empty
• PD:
  closed-set identification (biometric application)
application that ranks the biometric references in the enrolment database in order of decreasing similarity against a recognition biometric sample
NOTE 1 Closed-set identification always returns a non-empty candidate list
NOTE 2 Closed-set identification is rarely used within practical systems, but is often used experimentally

Argument: there is a claim that John is most similar to John. Thus there is a claim, thus this concept is inconsistent.

**CN: mate**
• Two biometric samples
• Same biometric subject, some biometric characteristic
• PD: mate

**CN: associative relation**
Characteristics developed by WG1
Characteristics need further development by WG1
CN Concept name
PD Preliminary designation
• Essential characteristic
### C.11.11 Performance 11

#### CN: Performance metrics
- **PD:**
  - Editor’s note: was this meant to be a concept, or just the sub-field name?

#### CN: Failure to process
- **PD:**

#### CN: Receiver operation characteristics (ROC)
- **PD:**

#### CN: Detection error trade-off (DET)
- **PD:**

#### CN: False rejection
- **PD:**
  - Genuine verification transaction error
  - Genuine claim
  - The system’s decision process fails to confirm the claim
  - NOTE Includes failure to acquire adequate features

From Kyoto meeting. We need:
- Failure to process (i.e. feature extraction returns an error)
- Failure to enrol
- Failure to create usable [probe]

#### CN: False acceptance
- **PD:**
  - Impostor verification transaction error
  - Impostor claim
  - The system’s decision process falsely confirms the claim

Final thoughts in London: Need to define difference between BioAPI Verify and BioAPI Identify. Need to determine if false match rate is dependent on database size. Maybe need a second term – one for dependent, one for independent.

Berlin Note: Simply appearing on a candidate list is not a false match.

#### CN: False reject rate
- **PD:**
  - Proportion of genuine verification transactions falsely rejected

WG5 defn: proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed

#### CN: Equal error rate
- **PD:**
  - Note: This was added in response to CDN comment, but may have been deleted during discussion on this topic. Discuss in Kyoto if concept needed here.

#### CN: False acceptance rate
- **PD:**

#### CN: False reject rate
- **PD:**
  - Proportion of impostor verification transactions falsely accepted

WG5 defn: proportion of verification transactions with truthful claims of identity that are incorrectly denied
C.12 Quality

acquisition fidelity fidelity of a sample attributable to the acquisition process
Attributes inherent characteristics of the source from which a biometric sample is derived that may affect the character of the biometric sample
Character contributor to quality of a sample attributable to inherent features of the source (ie. attributes)
environmental physical surroundings and conditions where biometric capture occurs, including operational factors such as operator skill and enrollee cooperation level
extraction fidelity the component of the fidelity of a sample attributable to the biometric feature extraction process
Extrinsic when used to describe a quality score, requiring reference to an external source, such as a standard, register, or technical specifications for full interpretation and normalisation
Fidelity the degree of similarity between a biometric sample and its source Note: the fidelity of a sample is comprised of individual components of fidelity attributed to each step through which it is Processed
Improvability the degree to which the predicted utility of a biometric sample can be improved upon through recapture or image enhancement techniques
Intrinsic when used to describe a quality score, conveying fully interpreted, normalised data without the requirement for additional extrinsic information for normalisation
Interpretation the process of analyzing a quality score along with other data in order to give that score contextual, relative meaning
Mate a biometric sample belonging to a set of biometric samples of the same biometric type and derived from the same source
observed sample false accept rate (osFAR) the rate at which an individual biometric sample falsely matches to other samples in a dataset Note: comparator performance is dependent on the quality of both samples being compared and on the comparator used
observed sample false reject rate (osFRR) the rate at which an individual biometric sample falsely fails to match other mates in a dataset Note: comparator performance is dependent on the quality of both samples being compared and on the comparator used
Operator the individual who processes a user in a biometric system, performing or supervising capture and recapture
peak signal to noise ratio (PSNR) a metric used to express the pixel-to-pixel similarity between two digital images, where differences are typically introduced by some image processing such as compression
Performance an assessment of the TAR, TRR, FAR, FRR, FTA, and FTE of a biometric system
predicted sample false accept rate (psFAR) the rate at which an individual biometric sample is expected to falsely match other samples Note: comparator performance is dependent on the quality of both samples being compared (the search data and the file data), and on the comparator used
predicted sample false reject rate (psFRR) the rate at which an individual biometric sample is expected to falsely fail to match other mates in a dataset. Note: comparator performance is dependent on the quality of both samples being compared (the search data and the file data), and on the comparator used
Quality the degree to which a biometric sample fulfils its specified requirements for its targeted application
quality score a quantitative expression of the utility, or predicted performance of a biometric sample in a comparison environment
quality score normalisation to cause the quality assessment algorithm to produce a score that conforms to a quality standard or norm so that there is consistency in the way the quality score is interpreted
quality score normalisation dataset (QSND) a dataset of biometric samples annotated with quality scores that attempt to be predictive of the contribution of the sample to the overall performance of a comparator or class of comparators Note: such assignment might be derived from the results of controlled performance tests
quality score percentile rank (QSPR) the percentile rank of the quality score of a biometric sample, derived from its own utility score and those of other samples in an identified control dataset (see QSND)
raw quality score a quality score that has not been interpreted, either by the creator or recipient of the score, and alone may not intrinsically provide contextual information
Sample an image, signal, or pattern based interpretation of a physical human feature used for identification or verification using biometric techniques
signal processing fidelity component of the fidelity of a sample attributable to the signal processing process
signal processing fidelity score (SPFS) an objective, relative, quantified expression of the Signal processing Fidelity of an image-based biometric sample
Source the physical body part or function represented by a biometric sample
Utility the observed performance of a sample in a biometric system, or similarly the impact of an individual biometric sample on the overall performance of a biometric system. The character of the sample source and the fidelity of the processed samples contribute to—or similarly detract from—the utility of the sample
Annex D
(informative)

Priority terms list

The following terms represent the list of concepts that appear in developing SC37 documents. This list has been extracted from the 2004-11 WG2/3-to-WG1 liaison report. The following list is modified from the original report in that the list is ordered according to the number of times it appears in SC37 documents.

This list is to be used for SD2 development purposes and is meant to provide WG1 members with an indication of which concepts should be developed first. Note that concepts are developed within WG1 by concept map, and not term-by-term. As such the concept map containing the most high priority terms according to the list below will be worked on first, then the concept map with the next most high priority terms, and so on.

This Annex will be removed from SD2 once all concepts in the list have been developed within WG1.

Editor's note: request that National Bodies do not comment on this list directly. It is simply for information purposes during concept development and will not be maintained within SD2. Please use the list when making comments on which concept maps should be developed first by WG1 at the South Africa meeting. Other comments that may arise from this list are concepts noted here, which are deemed essential to a particular concept map, but are not currently represented in the relevant concept map. As such, comments should be made in the vein of adding a concept to a particular concept map.

Table D.1 — Priority term list as derived from SC37 documents

<table>
<thead>
<tr>
<th>TERMS USED IN SC37 DOCUMENTS</th>
<th># OF SC37 DOCS TERM APPEARS IN</th>
<th>RELEVANT CONCEPT MAP</th>
<th>TERMS USED IN SC37 DOCUMENTS</th>
<th># OF SC37 DOCS TERM APPEARS IN</th>
<th>RELEVANT CONCEPT MAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>biometric sample</td>
<td>13</td>
<td>Biometric data</td>
<td>down-sample</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric</td>
<td>11</td>
<td>General concepts</td>
<td>encrypt/encryption</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric data</td>
<td>9</td>
<td>Biometric data</td>
<td>enrolment attempt</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric system</td>
<td>9</td>
<td>Biometric system components</td>
<td>enrolment attempt limit</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometrics</td>
<td>9</td>
<td>General concepts</td>
<td>enrolment presentation</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>enrolment</td>
<td>9</td>
<td>Interacting / Functioning</td>
<td>enrolment presentation limit</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>capture</td>
<td>8</td>
<td>Interacting</td>
<td>enrolment sequence</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>identification</td>
<td>8</td>
<td>Functioning</td>
<td>enrolment sequence limit</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>verification</td>
<td>8</td>
<td>Functioning</td>
<td>Equal Error Rate (EER)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>core</td>
<td>7</td>
<td>experimenter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>false accept rate (false acceptance rate)</td>
<td>7</td>
<td>Performance</td>
<td>extraction (feature extraction)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>false reject rate (false rejection rate)</td>
<td>7</td>
<td>Performance</td>
<td>face biometrics</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>match</td>
<td>7</td>
<td>Non-biometric data</td>
<td>Facial Animation Parameter (FAP)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>comparison</td>
<td>6</td>
<td>Functioning</td>
<td>facial image</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>identify</td>
<td>6</td>
<td>Application</td>
<td>facial image type</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>matching</td>
<td>6</td>
<td>Functioning</td>
<td>failure to enrol</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>template</td>
<td>6</td>
<td>Biometric data</td>
<td>failure-to-acquire-rate</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric template</td>
<td>5</td>
<td>Biometric data</td>
<td>failure-to-enrol rate</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>claimant</td>
<td>5</td>
<td>Personnel</td>
<td>fallback</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
| intermediate biometric sample | 5 | Biometric data | fallback procedures and systems | 1 |&
| processed biometric sample  | 5                               | Biometric data       | false claim                  | 1                              |
| raw biometric sample        | 5                               | Biometric data       | false match rate (FMR)       | 1                              |
| user                        | 5                               | Biometric data       |                             |                                |
| verify                      | 5                               | Application          | false-negative identification-error rate | 1 |

82 © ISO/IEC 2006 – All rights reserved
<table>
<thead>
<tr>
<th>application</th>
<th>4</th>
<th>Application</th>
<th>4</th>
<th>identification-error rate</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>biometric data block (BDB)</td>
<td>4</td>
<td>Application</td>
<td>4</td>
<td>feature point</td>
<td>1</td>
</tr>
<tr>
<td>biometric information record (BIR)</td>
<td>4</td>
<td>features</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>database</td>
<td>4</td>
<td>Personnel</td>
<td>4</td>
<td>final test result code</td>
<td>1</td>
</tr>
<tr>
<td>end user</td>
<td>4</td>
<td>filtering</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>extraction</td>
<td>4</td>
<td>finger geometry</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>false non match rate (FNMR)</td>
<td>4</td>
<td>finger pattern</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>one-to-one</td>
<td>4</td>
<td>Functioning</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>one-to-many</td>
<td>4</td>
<td>fingerprint biometrics</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>resolution</td>
<td>4</td>
<td>fingerprint image area</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>score</td>
<td>4</td>
<td>Non-biometric data</td>
<td>4</td>
<td>fraudulent claim</td>
<td>1</td>
</tr>
<tr>
<td>threshold</td>
<td>4</td>
<td>Non-biometric data</td>
<td>4</td>
<td>f-resolution</td>
<td>1</td>
</tr>
<tr>
<td>attempt</td>
<td>3</td>
<td>Interacting</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication</td>
<td>3</td>
<td>Application</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>base standard</td>
<td>3</td>
<td>fusion</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>biometric product</td>
<td>3</td>
<td>Biometric system components</td>
<td>3</td>
<td>genuine attempt</td>
<td>1</td>
</tr>
<tr>
<td>cell</td>
<td>3</td>
<td>genuine claim</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>delta</td>
<td>3</td>
<td>grayscale image</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>encryption</td>
<td>3</td>
<td>hand geometry (hand identification)</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>enrollee</td>
<td>3</td>
<td>handle</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>false accept (false acceptance)</td>
<td>3</td>
<td>Performance</td>
<td>3</td>
<td>human examination</td>
<td>1</td>
</tr>
<tr>
<td>false reject (false rejection)</td>
<td>3</td>
<td>Performance</td>
<td>3</td>
<td>identification application</td>
<td>1</td>
</tr>
<tr>
<td>live capture</td>
<td>3</td>
<td>Interacting</td>
<td>3</td>
<td>identification rank</td>
<td>1</td>
</tr>
<tr>
<td>negative identification</td>
<td>3</td>
<td>Application</td>
<td>3</td>
<td>identification rate (true positive)</td>
<td>1</td>
</tr>
<tr>
<td>one-to-few</td>
<td>3</td>
<td>Functioning</td>
<td>3</td>
<td>identification system</td>
<td>1</td>
</tr>
<tr>
<td>record</td>
<td>3</td>
<td>image</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>population</td>
<td>3</td>
<td>Personnel</td>
<td>3</td>
<td>image resolution</td>
<td>1</td>
</tr>
<tr>
<td>positive identification</td>
<td>3</td>
<td>Application</td>
<td>3</td>
<td>implementation under test (IUT)</td>
<td>1</td>
</tr>
<tr>
<td>record</td>
<td>3</td>
<td>图像</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>reference template</td>
<td>3</td>
<td>Biometric data</td>
<td>3</td>
<td>initial enrolment</td>
<td>1</td>
</tr>
<tr>
<td>registration</td>
<td>3</td>
<td>Natural language</td>
<td>3</td>
<td>interchange format</td>
<td>1</td>
</tr>
<tr>
<td>template adaptation</td>
<td>3</td>
<td>Functioning</td>
<td>3</td>
<td>standard/standard</td>
<td>1</td>
</tr>
<tr>
<td>transaction</td>
<td>3</td>
<td>interface systems</td>
<td>3</td>
<td>interchange format</td>
<td>1</td>
</tr>
<tr>
<td>validation</td>
<td>3</td>
<td>Natural language</td>
<td>3</td>
<td>intermediate behavioral data</td>
<td>1</td>
</tr>
<tr>
<td>valley</td>
<td>3</td>
<td>iris</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>adaptation</td>
<td>2</td>
<td>Functioning</td>
<td>2</td>
<td>level 0</td>
<td>1</td>
</tr>
<tr>
<td>API (Application Programming Interface)</td>
<td>2</td>
<td>level I</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BDB format identifier</td>
<td>2</td>
<td>level II</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>biometric algorithm</td>
<td>2</td>
<td>level III</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>biometric identification</td>
<td>2</td>
<td>Functioning</td>
<td>2</td>
<td>limbus</td>
<td>1</td>
</tr>
<tr>
<td>biometric information</td>
<td>2</td>
<td>line pair (lp)</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric Information Record (BIR)</td>
<td>2</td>
<td>live-scan print</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>biometric product identifier</td>
<td>2</td>
<td>match attempt limit</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>biometric product owner</td>
<td>2</td>
<td>match on card</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>biometric profile</td>
<td>2</td>
<td>match presentation</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>biometric verification</td>
<td>2</td>
<td>Functioning</td>
<td>2</td>
<td>match sequence</td>
<td>1</td>
</tr>
<tr>
<td>bit-depth</td>
<td>2</td>
<td>match sequence limit</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CBEFF biometric organization</td>
<td>2</td>
<td>match template</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CBEFF biometric organization identifier</td>
<td>2</td>
<td>minimal spatial wavelength</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CBEFF patron</td>
<td>2</td>
<td>Modal User Interface</td>
<td>1</td>
<td>Biometric data</td>
<td></td>
</tr>
<tr>
<td>CBEFF patron format</td>
<td>2</td>
<td>model</td>
<td>1</td>
<td>multi-biometric</td>
<td></td>
</tr>
<tr>
<td>continuous tone image</td>
<td>2</td>
<td>monomodal</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>decision</td>
<td>2</td>
<td>Functioning</td>
<td>multi-biometric</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>dimension</td>
<td>2</td>
<td>multi-biometric authentication</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>failure to acquire</td>
<td>2</td>
<td>multi-factor authentication</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>friction ridge</td>
<td>2</td>
<td>multi-instance</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>grayscale</td>
<td>2</td>
<td>MultiModal DELETE</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>identifier</td>
<td>2</td>
<td>multi-modal DELETE</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>identity</td>
<td>2</td>
<td>Personnel</td>
<td>multimodality</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>impostor</td>
<td>2</td>
<td>multiple biometric</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>matching score</td>
<td>2</td>
<td>Non-biometric data</td>
<td>negative claim by the source</td>
<td>1</td>
<td>Interacting</td>
</tr>
<tr>
<td>minuita (single)</td>
<td>2</td>
<td>non-commuting bins</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>minutiae (pl)</td>
<td>2</td>
<td>non-commuting bins</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multi-modal</td>
<td>2</td>
<td>General concepts</td>
<td>observer</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>operator</td>
<td>2</td>
<td>Personnel</td>
<td>offline testing</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>presentation</td>
<td>2</td>
<td>online testing</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>reference BiR</td>
<td>2</td>
<td>Biometric data (category, but does not appear on concept map)</td>
<td>open-set identification</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ridge bifurcation</td>
<td>2</td>
<td>operational evaluation</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ridge ending</td>
<td>2</td>
<td>packed data format</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sample</td>
<td>2</td>
<td>pad</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sample BiR</td>
<td>2</td>
<td>Biometric data (category, but does not appear on concept map)</td>
<td>palm biometrics</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>scoring</td>
<td>2</td>
<td>passive attack</td>
<td>1</td>
<td>Interacting</td>
<td></td>
</tr>
<tr>
<td>skeleton</td>
<td>2</td>
<td>payload</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>token</td>
<td>2</td>
<td>pen azimuth</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>absolute interoperability</td>
<td>1</td>
<td>pen elevation</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>abstract test suite</td>
<td>1</td>
<td>pen rotation</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>accessibility</td>
<td>1</td>
<td>pen tilt along the x-axis</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>active attack</td>
<td>1</td>
<td>Interacting</td>
<td>pen tilt along the y-axis</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>adaptation (template adaptation)</td>
<td>1</td>
<td>Functioning</td>
<td>penetration rate</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>administrator</td>
<td>1</td>
<td>Personnel</td>
<td>personal data protection</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>algorithm</td>
<td>1</td>
<td>pixels per centimeter (ppcm)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>application class</td>
<td>1</td>
<td>pixels per inch (ppi)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>assertion</td>
<td>1</td>
<td>pixels per millimeter (ppmm)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>assertion identifier</td>
<td>1</td>
<td>plain fingerprint image</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>assertion test</td>
<td>1</td>
<td>point jitter</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>asynchronous</td>
<td>1</td>
<td>portrait</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>attach session</td>
<td>1</td>
<td>positive claim by the source</td>
<td>1</td>
<td>Interacting</td>
<td></td>
</tr>
<tr>
<td>attack</td>
<td>1</td>
<td>Interacting</td>
<td>presentation effects</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>attended operation</td>
<td>1</td>
<td>privacy</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>authenticate</td>
<td>1</td>
<td>Application</td>
<td>pupil</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>BDB format</td>
<td>1</td>
<td>quasi-governmental institutions</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BDB format owner</td>
<td>1</td>
<td>raw</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>binary large object (BLOB)</td>
<td>1</td>
<td>raw biometric data</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>binning</td>
<td>1</td>
<td>raw data</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>binning error</td>
<td>1</td>
<td>raw fingerprint image</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BioAPI</td>
<td>1</td>
<td>receiver operating characteristic curve</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BioAPI component</td>
<td>1</td>
<td>red-eye</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BioAPI Function Provider</td>
<td>1</td>
<td>re-enrolment</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BioAPI Unit</td>
<td>1</td>
<td>register</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>biometric authentication</td>
<td>1</td>
<td>Application</td>
<td>registrar</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric behavioral data</td>
<td>1</td>
<td>Biometric data</td>
<td>registration authority</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric characteristic</td>
<td>1</td>
<td>Biometric data</td>
<td>relative interoperability</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>---</td>
<td>----------------</td>
<td>---------------------------</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>biometric data type</td>
<td>1</td>
<td>Devices</td>
<td>relevant ISO/IEC Subcommittee</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric device</td>
<td>1</td>
<td>Devices</td>
<td>remote access policy</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric feature</td>
<td>1</td>
<td>Biometric data</td>
<td>repeated instance</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric feature data unit</td>
<td>1</td>
<td>Biometric data</td>
<td>re-sampling</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric feature extraction</td>
<td>1</td>
<td>Biometric data</td>
<td>retinal biometrics</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric functions</td>
<td>1</td>
<td>Functioning</td>
<td>ridge skeleton endpoint</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric identification data</td>
<td>1</td>
<td>Biometric data</td>
<td>rolled fingerprint image</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric image data</td>
<td>1</td>
<td>Biometric data</td>
<td>round</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Biometric Information Template (BIT)</td>
<td>1</td>
<td>Biometric data</td>
<td>sampling frequency</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric matching algorithm</td>
<td>1</td>
<td>Biometric data</td>
<td>scan resolution</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric measure</td>
<td>1</td>
<td>Biometric data</td>
<td>scenario evaluation</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric model</td>
<td>1</td>
<td>Biometric data</td>
<td>scenario script</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric opaque data block (BD0)</td>
<td>1</td>
<td>Biometric data</td>
<td>sclera</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Biometric Policy (BP)</td>
<td>1</td>
<td>Biometric data</td>
<td>self-contained device</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Biometric Practice Statement (BSP)</td>
<td>1</td>
<td>Biometric data</td>
<td>sensor</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric reference template</td>
<td>1</td>
<td>Biometric data</td>
<td>signature (digital signature)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric sensor</td>
<td>1</td>
<td>Biometric data</td>
<td>signature verification biometrics</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric sensor device</td>
<td>1</td>
<td>Biometric data</td>
<td>simple CBEFF BIR structure</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric system components</td>
<td>1</td>
<td>Biometric data</td>
<td>single factor authentication</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric transformation</td>
<td>1</td>
<td>Biometric data</td>
<td>societal aspects</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric type</td>
<td>1</td>
<td>Biometric data</td>
<td>source BIR</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>biometric verification data</td>
<td>1</td>
<td>Biometric data</td>
<td>source/generator</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>BIP model system</td>
<td>1</td>
<td>Biometric data</td>
<td>standard biometric header (SBH)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>BIP real system</td>
<td>1</td>
<td>Biometric data</td>
<td>standardized interchange format instance</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>callback</td>
<td>1</td>
<td>Biometric data</td>
<td>subject (data)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>candidate</td>
<td>1</td>
<td>Biometric data</td>
<td>sufficiency</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>candidate list</td>
<td>1</td>
<td>Biometric data</td>
<td>supplying entity</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>CBEFF</td>
<td>1</td>
<td>Biometric data</td>
<td>synchronous</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>CBEFF patron format identifier</td>
<td>1</td>
<td>Biometric data</td>
<td>system</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>CBEFF patron identifier</td>
<td>1</td>
<td>Biometric data</td>
<td>system description</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>CBEFF root header</td>
<td>1</td>
<td>Biometric data</td>
<td>system implementer</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>CBEFF sub-header</td>
<td>1</td>
<td>Biometric data</td>
<td>system operator</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>cell quality group</td>
<td>1</td>
<td>Biometric data</td>
<td>system under test (SUT)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>cell structure</td>
<td>1</td>
<td>Biometric data</td>
<td>target BIR</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>certification</td>
<td>1</td>
<td>Biometric data</td>
<td>target population</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>channel</td>
<td>1</td>
<td>Biometric data</td>
<td>taxonomy</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>channel effects</td>
<td>1</td>
<td>Biometric data</td>
<td>technology evaluation</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>chin</td>
<td>1</td>
<td>Biometric data</td>
<td>test case</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>claim</td>
<td>1</td>
<td>Biometric data</td>
<td>test method implementation</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>claim of identify</td>
<td>1</td>
<td>Biometric data</td>
<td>test organization</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>closed-set identification</td>
<td>1</td>
<td>Biometric data</td>
<td>test report</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>color image</td>
<td>1</td>
<td>Biometric data</td>
<td>test result code</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>color space</td>
<td>1</td>
<td>Biometric data</td>
<td>test subject</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>combination</td>
<td>1</td>
<td>Biometric data</td>
<td>time series</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>common biometrics exchange formats framework (CBEFF)</td>
<td>1</td>
<td>Biometric data</td>
<td>TLV encoding</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>complex CBEFF BIR structure</td>
<td>1</td>
<td>Biometric data</td>
<td>true claim</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>complex true CBEFF BIR structure</td>
<td>1</td>
<td>Biometric data</td>
<td>interacting</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>component registry</td>
<td>1</td>
<td>type I error</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>---</td>
<td>--------------</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component Registry Services (CRS)</td>
<td>1</td>
<td>type II error</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>confidence interval</td>
<td>1</td>
<td>typeline</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>confidentiality</td>
<td>1</td>
<td>Uni-Modal DELETE</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>conformance</td>
<td>1</td>
<td>valley bifurcation</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>conformity assessment</td>
<td>1</td>
<td>variance (V)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cross-jurisdictional aspects</td>
<td>1</td>
<td>vendor</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>crown</td>
<td>1</td>
<td>verification application</td>
<td>Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cumulative match characteristic curve</td>
<td>1</td>
<td>verification system</td>
<td>Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>decision (identification decision)</td>
<td>1</td>
<td>verifier/matcher</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>decision (verification decision)</td>
<td>1</td>
<td>voice biometrics</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>decision policy</td>
<td>1</td>
<td>x-resolution</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>defrauder claim</td>
<td>1</td>
<td>Interacting</td>
<td>x-size</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>detection error trade-off curve</td>
<td>1</td>
<td>y-resolution</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>disrupter</td>
<td>1</td>
<td>Personnel</td>
<td>y-size</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>domain of use</td>
<td>1</td>
<td>zero-effort impostor attempt</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dots per inch (DPI)</td>
<td>1</td>
<td>z-resolution</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>z-size</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Bibliography


Alphabetical Index

[physical features that impact data capture conditions, 11
acceptance, 7
active attack, 14
affirmed biometric claim, 14
aggregated biometric data, 8
anonymised biometric data, 8
anonymous biometric data, 8
applicant, 22
application, 16
attract, 14
attend, 16
attendant, 16
attended operation, 14
authenticate, 22
authentication, 17
biometric, 2
biometric algorithm, 2
biometric application decision, 9
biometric capture device, 8
biometric capture process, 11
biometric capture subject, 15
biometric capture subsystem, 11
biometric characteristic, 4
biometric claim, 14
biometric data, 4
Biometric Data Block (BDB), 4
biometric data log, 7
biometric data subject, 15
biometric enrolment database, 3
biometric failure to enrol, 18
biometric failure to enrol rate, 18
biometric feature, 4
biometric feature extraction process, 13
biometric identification (biometric system function), 9
biometric identification application, 17
Biometric Information Record (BIR), 4
biometric match trial (previously referred to as, 18
biometric modality, 2
biometric mode (noun), model (adj), 2
biometric model, 5
biometric non-match trial (previously referred to as, 18
biometric product, 3
biometric property, 4
biometric recogniser, 17
biometric reference, 4
biometric reference adaptation, 12
biometric reference identifier, 6
biometric reference renewal, 12
biometric sample, 5
biometric sample metadata, 7
biometric system, 3
biometric system operator, 16
biometric system owner, 16
biometric template, 5
biometric verification (biometric application), 17
biometric verification (biometric system function), 9
biometrics, 3
candidate, 6
candidate list, 6
candidate score, 6
capture, 22
capture (function call), 11
capture medium, 8
capture tool, 8
captured biometric sample, 5
claimant, 16
claimed identity, 7
closed set combination identification error, 19
closed set false-negative identification error, 19
closed set false-negative identification error rate, 19
closed set identification error, 19
closed set identification error trials, 19
closed-set identification, 17
combined identification error, 21
comparison, 9
comparison decision, 6
comparison score, 6
effective presentation, 11
data capture conditions, 8
data object, 3
database, 23
deactivate, 11
dealer policy, 7
decryption, 13
de-enrollment, 12
denied biometric claim, 14
detection error trade-off (DET), 19
direct capture device, 8
distance score / dissimilarity score, 6
duplicate enrolment check, 12
encryption, 13
end result of enrolment, 12
end user, 16
enrol, 13
enrollee, 16
enrolment, 13
enrolment data record, 3
equal error rate, 19
enrolled presentation, 12
failure to acquire, 19
failure to acquire rate, 19
failure to acquire rate for enrolment, 19
failure to capture, 20
failure to process, 20
take accept / acceptance, 20
take accept rate, 20
false match, 20
false match rate, 20
false non-match, 20
false non-match rate, 20
take reject / rejection, 21
take reject rate, 21
false-negative open set identification error, 21
false-negative identification error, 19
false-negative open set identification error rate, 21
false-positive identification error, 19
false-positive open set identification error, 21
translucent biometric claim, 14
transient presentation, 12
genuine verification attempt, 14
genuine verification transaction, 15
ground truth, 7
identify, 17
identity concealer, 16
impersonate presentation, 12
impostor, 16
imposter verification attempt, 14
imposter verification transaction, 15
indirect capture device, 8
individual, 23
  individual metadata, 7
  individualisable anonymised biometric data, 8
  instructions and subject feedback, 11
intermediate biometric sample, 5
intermediate biometric sample processing, 13
  Intermediate media transformer, 9
inter point of transaction, 11
inter side presentation, 12
live capture, 15
leading biometric reference, 11
match (n), 6
  matching score, 7
multibimetric, 2
multialgorithmic, 2
multimodal, 2
multimodal processing, 2
multimodal sensor, 2
negative biometric claim, 15
negative identification, 17
non-match (n), 7
non-individualisable anonymised biometric data, 8
one-to-few, 10
one-to-many search, 10
one-to-one comparison, 10
open set false-negative identification error rate, 21
open set false-positive identification error rate, 21
open set identification error rate, 21
open set identification error trials (matched), 21
open set identification error trials (no match), 21
open-set identification (biometric application), 18
  passage attack, 14
  positive biometric claim, 15
positive identification, 9, 18
  presentation, 11, 15
  probe (enrolled) / recognition biometric sample, etc, 5
processing device, 9
re-enrolment, 13
re-identification, 9, 18
registration, 13, 23
rejection, 7
right side presentation, 12
score, 23
scoring, 23
session, 9
session, 15
similarity score, 6
special treatment, 18
subject, 23
subject interface, 12
subversive capture subject, 16
subversive user, 15
system, 24
threshold, 7
thresholding / cull / exclude, 10
transducer, 15
trial, 15
uncooperative presentation, 12
unimodal, 2
user, 16
validation, 24
verification (biometric system function), 9
verification system, 3
verify, 24